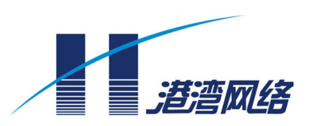
UniWorks UAS 用户手册

第一部分　　安装 **UniWorks UAS** 系统

第二部分　　配置 **UniWorks UAS** 系统



UniWorks UAS 用户手册

资料编号　P-18080022-20040420-100
产品版本　V1.00
资料状态　发行

手册使用说明

读者对象

本手册的读者对象为安装和使用 UniWorks UAS（UAS，统一访问服务器，是 Uni-Access Server 的缩写）系统进行认证、授权和计费等业务管理的系统管理员。本手册需要读者熟悉以太网和组建局域网的概念和术语。

内容介绍

本手册详细介绍了 UniWorks UAS 系统的安装和使用方法，是系统管理人员了解本系统并顺利完成系统安装与使用的指导文档。《UniWorks UAS 用户手册》共分为两个部分：

第一部分 安装

通过阅读本部分内容，用户将对本系统的用途、特点和版本信息等有一个全面的了解，并可进行本系统的正确安装。具体包括以下内容：

章序号	题目	内容描述
第1章	UniWorks UAS系统概述	简要讲述UniWorks UAS系统的功能、特点及版本说明。
第2章	系统构建	讲述UniWorks UAS系统的运行环境构建和安装、卸载方法。

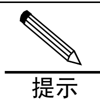
第二部分 配置

通过阅读本部分内容，用户将了解使用本系统的相关知识，并可利用本系统完成认证、授权和计费等业务管理。具体包括以下内容：

章序号	题目	内容描述
第3章	相关知识	讲述与使用本系统相关的网络基本知识及其它专业知识。
第4章	系统启动	介绍系统后台服务和管理服务器的组成、功能，以及如何启动它们，并进入管理系统。
第5章	服务器配置	讲述AAA服务器、Portal服务器、DHCP服务器和管理服务器的基本配置，如IP地址和密钥等。
第6章	AAA服务器管理	讲述AAA服务器管理的相关原理和配置。
第7章	Portal服务器管理	讲述Portal服务器管理的相关原理和配置。
第8章	DHCP服务器管理	讲述DHCP服务器管理的相关原理和配置。
第9章	用户管理	讲述用户管理的相关操作。
第10章	安全管理	讲述安全管理的相关原理和配置。
附录	常见问题处理	讲述UniWorks UAS系统在使用中可能会遇到的问题及处理方法。

手册约定

手册中有关图标的约定如下：

图标	说明
注意	这个图标表示提醒用户注意事项。
 提示	这个图标主要给出一些与正文相关的信息，同时给用户一些指引，协助用户更好的理解正文的内容。

获取技术支援

港湾网络有限公司建立了以总部技术支援中心、区域技术支援中心和本地技术支援中心为主体的完善的三级服务体系，并提供全天候 24 小时×365 天的电话热线服务。客户在产品使用及网络运行过程中遇到问题时请随时与港湾网络有限公司各地方的服务支持热线联系。请客户到www.harbournetworks.com获取各地服务支持热线电话。此外，客户还可通过港湾网络有限公司网站及时了解最新产品动态，以及下载需要的技术文档。

目录

1 UniWorks UAS 系统概述

1.1 简介

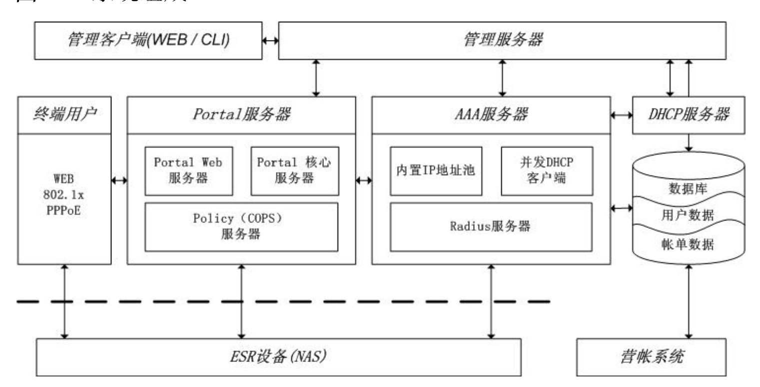
UniWorks UAS 系统是港湾网络有限公司推出的认证、授权和计费业务管理软件系统，包括 AAA（认证、授权、计费，是 Authentication、Authorization、Accounting 的缩写）服务器、DHCP 服务器、Portal 服务器和统一管理服务器共四部分。其中，AAA 服务器是 UniWorks UAS 系统的核心，实现对用户的认证、授权和计费功能；DHCP 服务器配合 AAA 服务器完成统一地址分配功能；Portal 服务器实现 Web 认证、用户 ACL 策略下发、内容服务计费以及灵活的业务拓展功能；管理服务器提供安全、可靠的管理人机接口，为系统管理员或远程管理用户提供方便、直观的操作管理界面，使用 Web 方式对 AAA 服务器、DHCP 服务器和 Portal 服务器进行统一的监控和配置。

UniWorks UAS 系统与 PowerHammer ESR 系列路由器等设备配合使用，可以实现 Web 用户及非 Web 用户的安全认证和计费管理。

1.1.1 系统组成

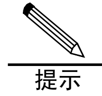
整个系统组成如图 1-1 所示：

图1-1 系统组成



其主要工作节点包括：

- 管理客户端（WEB/CLI）和管理服务器之间：系统管理员从 Web 游览器通过 HTTP、HTTPS 协议访问管理服务器或者通过命令行客户端访问管理服务器完成管理任务。可以同时有多个管理员进行操作。
- 管理服务器和 Portal 服务器、AAA 服务器、DHCP 服务器之间：管理服务器提供安全、可靠的管理人机接口，将系统管理员的管理操作转化为管理消息发送给 Portal 服务器、AAA 服务器和 DHCP 服务器，并把各服务器的响应结果反馈给系统管理员，从而对分布式结构的各个后台服务器实现统一方便的管理；
- Web /802.1x/PPPoE 用户与 Portal 服务器、ESR 设备（NAS）之间：ESR 设备（NAS）或 Portal 服务器接收到 Web/802.1x/PPPoE 用户的上线请求信息后，向 RADIUS 服务器发送认证请求；RADIUS 服务器对用户进行认证，并把认证结果返回 ESR 设备（NAS）或 Portal 服务器；如果认证通过，ESR 设备（NAS）或 Portal 服务器完成相应操作，允许用户接入；
- AAA 服务器与 DHCP 服务器之间：AAA 服务器与 DHCP 服务器配合，完成统一地址分配；
- AAA 服务器与数据库之间：完成相关信息的查询和记录，实现系统配置和用户计费等功能；
- 营帐系统与数据库之间：完成对用户帐单处理，实现系统营帐。


提示

目前， UniWorks UAS 系统 V1.00 版本暂不支持 CLI 方式的管理客户端；尚未实现营帐功能。

1.1.2 系统特点

1. 技术架构特点

- 分布式设计：组件化软件结构；系统可分布可集中，设置灵活
- 高性能：采用 Oracle9i 等专业数据库系统，支持大数据量，高并发度访问的高性能支持
- 高安全可靠性：双机热备，软件自动切换等技术手段；保证系统 7×24 小时不间断运行；HTTPS 支持、管理报文验证、IP 限制等多种技术手段保证数据的加密传输

- 良好的兼容性和扩展性：支持 Solaris 等多种专业 UNIX 平台；支持 Windows/Linux 等操作平台；充分考虑了业务及功能拓展性，保护用户投资

2. 业务功能特点

- 强大的策略配置下发功能（COPS 协议支持）
- 灵活的 Portal 业务拓展能力，支持页面内容个性化配置、业务计费等功能
- 多种认证方式的统一地址分配
- 与港湾网络有限公司的 PowerHammer ESR 系列路由器等设备配合，实现安全认证、实时 CUT 和端口反查等特色功能
- 提供丰富灵活的接口，可方便的与其它计费营帐系统对接

1.2 版本说明

UniWorks UAS 系统的 V1.00 版支持多操作系统平台的应用，可运行在 Solairs、Microsoft Windows2000/XP、Linux 等多种操作系统。可为各类型网络提供后台管理服务。


提示

本手册主要介绍 UniWorks UAS 系统 V1.00 的 Solairs 版和 Windows 版。

UniWorks UAS 系统的 V1.00 版本支持的设备种类包括：

- 港湾网络有限公司的 PowerHammer ESR 系列路由器等设备

主要支持的 Web 及非 Web 用户的业务管理功能包括：

- 认证
- 授权
- 计费

数据保存的基本方式包括：

- UniWorks UAS 系统数据库（MySql、Oracle 等），保存用户参数和计费数据等信息

UniWorks UAS 系统使用的主要 Socket 端口包括：

- RADIUS 服务器：端口 1812，1813(UDP)
- Portal 服务器：端口 443（HTTPS），80（HTTP），5656（TCP），5454（UDP），3288（COPS），10000（TCP），10001（TCP）
- 管理服务器：80（HTTP）


注意

如果这几个端口被其它应用程序使用，UniWorks UAS 系统将不能正常运行。

1.3 应用方式

1.3.1 非Web用户应用方式

非 Web 用户是指客户端采用 802.1x 或标准 PPPoE 客户端软件的用户。在这种应用方式下，终端客户采用 802.1x 或 PPPoE 客户端软件上网，需要安装、配置 AAA 服务器和管理服务器。Portal 服务器和 DHCP 服务器是可选的。


提示

1、如果不安装 Portal 服务器，系统将不拥有用户 ACL 下发、内容服务计费等高级功能;

2、不安装 DHCP 服务器，系统将不拥有统一 IP 地址分配功能。

1.3.2 Web用户和非Web用户混合应用方式

在这种应用方式下，终端客户可能使用普通 Web 浏览器作为客户端软件上网，也可能使用 802.1x 或 PPPoE 等客户端软件上网。在这种应用方式下，必须安装、配置 AAA 服务器、Portal 服务器以及管理服务器，DHCP 服务器可选。


提示

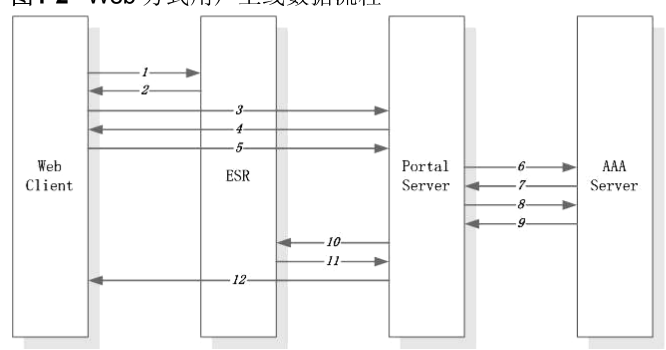
不安装 DHCP 服务器，系统将不拥有统一 IP 地址分配功能。

1.3.3 主要数据流程

1. Web 方式用户上线

Web 方式用户上线数据流程如下图所示：

图1-2 Web 方式用户上线数据流程



1）用户打开浏览器，输入欲访问的 URL，浏览器发送 HTTP 报文给 ESR 设备；

2）ESR 设备发现此用户尚未通过认证，则利用 HTTP 协议的 302 返回值，将用户的 HTTP 请求重定向到一个指向 Portal 服务器的新 URL 上；

- 此 URL 包含 Portal 服务器的地址，地址分配方式参数 readdr，NAS 地址参数 nasip，NAS 端口参数 nasport 等必要参数
- 为了数据的安全，新 URL 可以配置成 HTTPS 协议，保证终端用户和 Portal 服务器之间使用 HTTPS 协议通信

3）用户端浏览器用新 URL 访问 Portal 服务器；

4）Portal 服务器给用户返回一个包含用户名、密码输入框的登录页面；

5）用户填入正确的用户名、密码，然后，点击‘登录’按钮将这些信息提交给 Portal 服务器；

6）Portal 服务器根据用户输入的信息，构造 RADIUS 认证报文向 AAA 服务器发起认证；

7）AAA 服务器返回认证成功报文，并在报文中携带与此用户相关的一些属性。这些属性可能包括：

- 用户的上网权限属性（ACL）
- 用户的 IP 地址（如果是二次地址分配，AAA 在认证的同时会为用户分配一个 IP 地址）
- 用户的缺省网关，DNS 等（二次地址分配）

8）认证通过后，Portal 服务器紧接着向 AAA 服务器发起计费开始请求；

9）AAA 服务器确认计费开始；

10）Portal 服务器通过 COPS 协议通知 ESR 用户上线，并请求 ESR 为此用户设置上网权限（ACL）；

11）ESR 为此用户设置 ACL，并通过 COPS 协议给 Portal 服务器发回执，确认此用户上线；

12）Portal 服务器通过 HTTPS 协议给客户端浏览器返回一个上线成功页面。此页面中包含一个 OCX（如果是 IE 就调用 OCX，否则调用 Java Applet）小程序，用户上线计时信息和供用户正常下线的 URL 链接。如果系统配置成二次地址分配方式，页面中的 OCX 控件还负责将新分配的 IP 及缺省网关，DNS 等配置到用户的计算机上。

2. 非 Web 方式用户上线

非 Web 方式用户上线数据流程如下图所示：

图1-3 非 Web 方式用户上线数据流程

（1）用户打开 802.1x 或 PPPoE 客户端，输入用户名和密码进行登录；

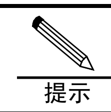
（2）ESR 设备根据用户的输入，组装 RADIUS 认证报文发送给 AAA 服务器；

（3）AAA 服务器认证通过，返回结果；

（4)ESR 设备通过 COPS 同步协议通知 Portal 服务器一个非 Web 用户上线成功；

（5）确认成功；

（6）ESR 设备通知客户端本次上线成功。

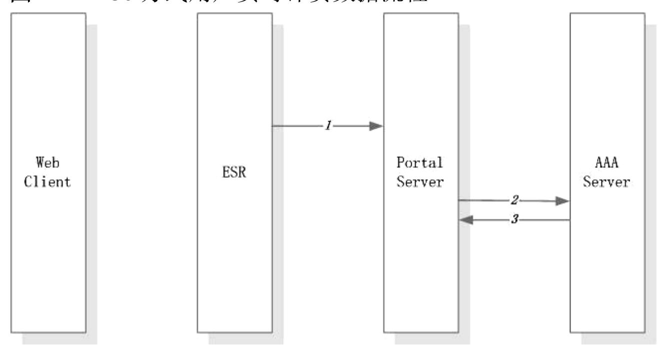

提示

如果只有非 Web 用户上线，系统中的 Portal 服务器可以不选，这样 4、5 两步流程也可取消。

3. Web 方式用户实时计费

Web 方式用户实时计费数据流程如下图所示：

图1-4 Web 方式用户实时计费数据流程



（1）用户如果配置了实时计费间隔，则在上线时会传给 ESR 设备，此后 ESR 设备会以此间隔为周期，定期通过 RADIUS 实时计费报文将用户的实时流量及时长等信息通过 COPS 协议通知 Portal 服务器；

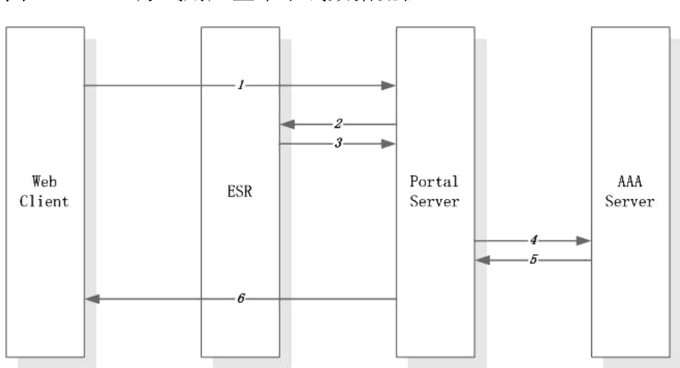
（2）Portal 服务器根据 ESR 设备传过来的实时信息向 AAA 服务器发送实时计费报文；

（3）AAA 服务器确认实时计费处理成功。

4. Web 方式用户正常下线

Web 方式用户正常下线数据流程如下图所示：

图1-5 Web 方式用户正常下线数据流程



（1）Web 终端用户点击在线小窗口中的“退出登陆”下线按钮或链接，向 Portal 服务器提交下线请求；

（2）Portal 服务器通过 COPS 协议请求 ESR 设备为此用户下线；

（3）ESR 设备确认下线成功，并将用户此时的流量等最新计费信息传过来；

（4）Portal 服务器组装停止计费报文发送到 AAA 服务器；

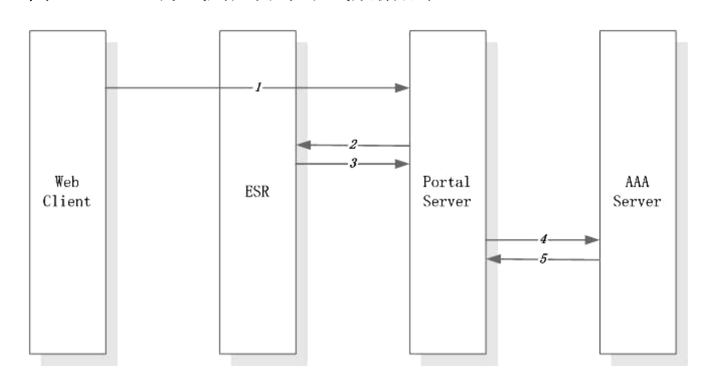
（5）AAA 服务器确认用户停止计费；

（6）Portal 服务器通知用户端浏览器，返回下线成功页面。

5. Web 方式用户异常下线（心跳信号检测）

Web 方式用户异常下线数据流程如下图所示：

图1-6 Web 方式用户异常下线数据流程



（1）用户上线后，页面中包含的小程序控件以一定的时间间隔向服务器通过 UDP 协议发送心跳信号；

（2）如果 Portal 服务器检测到一个 Web Client 已经 3 次没发送心跳信号了，就认为此用户已经异常。通过 COPS 协议请求设备此用户异常下线；

（3）ESR 设备确认异常下线成功；

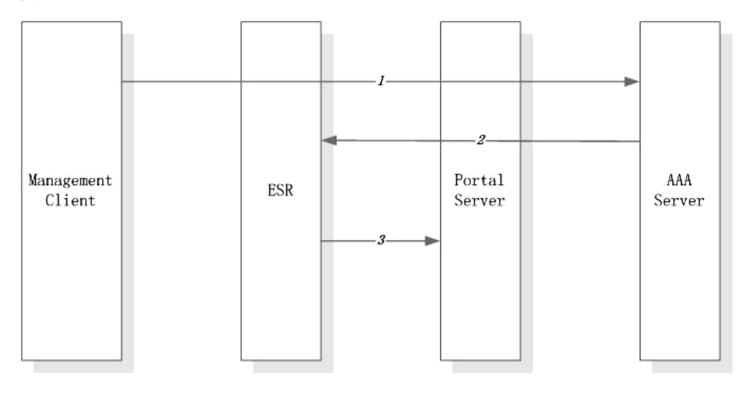
（4）Portal 服务器构造停止计费报文，发给 AAA 服务器；

（5）AAA 服务器确认停止计费成功。

6. 非 Web 方式用户强制下线（Radius CUT）

非 Web 方式用户强制下线数据流程如下图所示：

图1-7 非 Web 方式用户强制下线数据流程



（1）管理客户端（Web 或命令行程序）向 AAA 服务器发送请求 CUT 掉一个用户；

（2）AAA 服务器将此用户停止计费，并通过特定报文主动通知 ESR 设备此用户下线；

（3）ESR 设备确认此用户停止计费，通过 COPS 协议通知 Portal 服务器从 Session Pool 中删掉此用户。

2 系统构建

2.1 硬件环境

2.1.1 Windows版

UniWorks UAS 系统安装在 PC 服务器上，其硬件配置要求如下：

- CPU 频率不小于 1.5GHz
- 硬盘容量不小于 40G 字节
- 内存不小于 512M 字节
- 具有网络连接设备

建议配置：

- HP PC Server ML-350 XEON 2.4G
- 40G SCSIHD
- 1024M 内存
- 100/1000M 以太网卡

2.1.2 Solaris版

UniWorks UAS 系统安装在 Sparc 工作站上，其硬件配置要求如下：

- CPU 频率不小于 SPARC v9 1GHz
- 硬盘容量不小于 40G 字节
- 内存不小于 1G 字节
- 具有网络连接设备

建议配置：

- Sun Blade 2000 SPARC v9 1.2G CPU
- 73GSCSIHD

- 1024M 内存
- 1000M 以太网卡

2.2 软件环境

2.2.1 Windows版

系统的软件环境主要包括：

- 操作系统：Windows 2000 Server / Professional（Service Pack 4），Windows XP
- 数据库：MySql、Oracle 等

2.2.2 Solaris版

系统的软件环境主要包括：

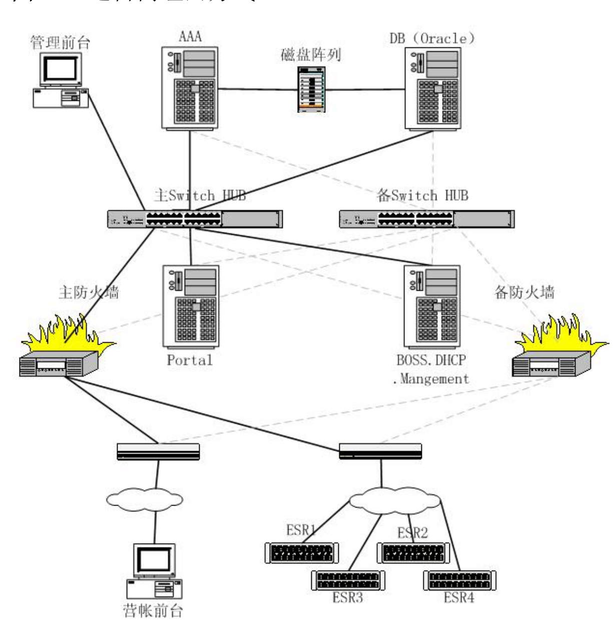
- 操作系统：Solaris 8/Solaris 9
- 数据库：MySql、Oracle 等

2.3 组网方式

2.3.1 运营商组网方式

UniWorks UAS 系统的运营商组网方式如下图所示：

图2-1 运营商组网方式



2. 软件配置

- Solaris 8/Solaris 9
- Veritas（双机备份软件）

3. 服务器配置

Sun Fire 280R server：

- 1.2GHz Ultra SPARC-III processors×2
- 8MB E-cache
- 8GB memory
- 73GB 10,000rpm HH internal FCAL disk drives×2

4. 各部分连接

- AAA 服务器、DB 数据库服务器、Portal 服务器、BOSS 营账系统、管理服务器和 DHCP 服务器（可选）等各个后台服务器分别运行在两套双机系统上，通过局域网组网连接，采用 TCP/IP 协议通信；
- 管理前台可采用 PC 机，通过局域网组网连接；

- 营帐前台需要通过 DDN/FRN 等上网；
- ESR 设备采用城域网组网连接，一套 UniWorks UAS 系统最多可支持 4 台 ESR 设备；
- 防火墙和 Switch HUB 都采用双套，以提高系统可靠性。一台防火墙占用 1 个公网 IP 地址。

5. 运行方式及分析

UniWorks UAS 系统采用两套双机主备方式运行：

- 小型机双机工作是不对称的，各自运行独立的应用程序，冷备份方式既保证可靠性，又可分担各小型机的负荷，保证系统性能；
- 正常情况下，主机 A 运行 AAA 服务器，主机 B 运行 DB 数据库服务器，主机 C 运行 Portal 服务器，主机 D 运行营帐服务器，管理服务器和 DHCP 可选组件；
- 数据库存储设备在高可靠的磁盘柜上；
- 在某个服务器发生故障的情况下，系统会自动切换进程到备服务器上。但是此时备服务器上运行的服务会增多（例如 Portal 服务器、BOSS 营账系统、管理服务器和 DHCP 服务器将运行在同一台小型机上），所以机器的资源负荷可能会很高，必要时可以采用一些管理措施降低小型机负荷。

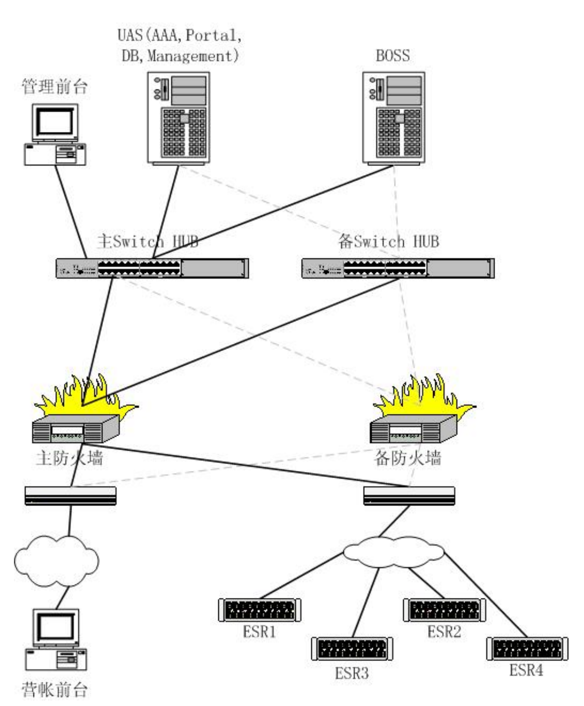
每台小型机都有两块网卡，当一块网卡不能工作时，另一块网卡将自动替换（特别地，如果某台 Switch HUB 不能工作时，与之相连的小型机的网卡也将自动倒换），并持有原网卡 IP。此时，新网卡将接入另一台 Switch HUB。由于两台 Switch HUB 是连接的，能保证两台 Switch HUB 有同样的输出/输出到防火墙。因此，两台 Switch HUB 是热备份的，无需人工干预。

防火墙是主备系统，当一台防火墙不能工作或与 Switch HUB 连接中断时，能自动倒换，从而保证始终有一套在工作。

2.3.2 企业网（教育网）组网方式

UniWorks UAS 系统的企业网（教育网）组网方式如下图所示：

图2-2 企业网（教育网）组网方式



2. 软件配置：

- Linux/Windows 2000 Server
- 可选用 Windows 2000 Cluster Service 或 Linux LVS 等双机软件增加系统可靠性

3. 服务器配置

- HP PC Server ML-350 XEON 2.4G
- 40G SCSIHD
- 1024M 内存
- 100/1000M 以太网卡

4. 各部分连接

- AAA 服务器、DB 数据库服务器、Portal 服务器、管理服务器和 DHCP 服务器（可选）等各个后台服务器运行在一台主机系统上，BOSS 营账系统运行在一台主机系统上，通过局域网组网连接，采用 TCP/IP 协议通信；
- 管理前台可采用 PC 机，通过局域网组网连接；

- 营帐前台需要通过 DDN/FRN 等上网；
- ESR 设备采用城域网组网连接，一套 UniWorks UAS 系统最多可支持 4 台 ESR 设备；
- 防火墙和 Switch HUB 都采用了双套，提高了可靠性。一台防火墙占用 1 个公网 IP 地址。

5. 运行方式及分析

UniWorks UAS 系统运行在两台服务器上

- UniWorks UAS 系统中的 AAA 服务器、DB 数据库服务器、Portal 服务器和管理服务器等运行在一台主机上；
- BOSS 营帐系统运行在另一台主机上；
- 可以选用 Windows 或 Linux 下的双机软件保证系统可靠性。

每台服务器都有两块网卡，当一块网卡不能工作时，另一块网卡将自动替换（特别地，如果某台 Switch HUB 不能工作时，与之相连的小型机的网卡也将自动倒换），并持有原网卡 IP。此时，新网卡将接入另一台 Switch HUB。由于两台 Switch HUB 是连接的，能保证两台 Switch HUB 有同样的输出/输出到防火墙。因此，两台 Switch HUB 是热备份的，无需人工干预。

防火墙是主备系统，当一台防火墙不能工作或与 Switch HUB 连接中断时，能自动倒换，从而保证始终有一套在工作。

2.4 UniWorks UAS系统安装

2.4.1 Windows版安装

UniWorks UAS 系统包括 AAA 服务器、DHCP 服务器、Portal 服务器和管理服务器四部分。用户可根据实际情况，有选择地进行安装。



提示

UniWorks UAS 系统的安装选择请参见 1.3 节的相关内容。

1. 安装准备

在安装本系统之前，如果需要安装 Portal 服务器或者管理服务器，为了支持 JSP 动态页面技术，必须确认系统已成功安装 j2sdk-1_4_0_03。安装方法是：运行软件光盘中提供的 j2sdk-1_4_0_03 安装程序，可按照提示进行安装。


注意

请将 UniWorks UAS 系统安装在磁盘空间比较大的路径下，因为在系统运行过程中，将有大量的数据存储在该路径下，需占用很大空间。建议磁盘可用空间大于 1G。

2. 安装 AAA 服务器

安装程序在光盘的“UniWorks\AAA”目录下，您可以直接运行光盘上“UniWorks\AAA”目录下的 setup.exe，或把 UniWorks 目录下的所有文件拷贝到本地，再运行“AAA”目录下的 setup.exe。主要安装过程描述如下：

1、 运行 setup.exe 后弹出 HarbourNetworks AAA Server 系统安装对话框；
2、 点击“Next”按钮，出现“许可证协议”窗口。用户必须认真阅读《港湾网络有限公司 AAA Server 软件产品最终用户使用许可协议》内容。用户确认同意协议内容请点击“Yes”按钮，进行下一步安装，弹出“选择目的地位置”对话框；点击“No”按钮则退出安装；
3、 在“选择目的地位置”对话框中，用户可通过“浏览”按钮选择系统安装路径，请确定所选路径下具有足够的磁盘空间。系统默认安装路径为“C:\Program Files\HarbourNetworks\SoftWare”。


提示

当多个系统安装在同一设备上的时候，第二个安装的软件不能选择路径。

4、 安装路径选好后，点击“下一步”按钮开始安装 HarbourNetworks AAA Server 系统，用户可以看到系统安装进度条，此步骤需要几分钟的时间（具体时间因 PC 服务器的硬件配置及软件系统的不同而略有差异）。
5、 系统安装[完成后，弹出“完成安装”对话框，提示用户是否立即重启计算机。用户可选择稍后重启计算机。此时用户点击“完成”按钮结束 HarbourNetworks AAA Server 系统的安装。

3. 安装 DHCP 服务器

安装程序在光盘的“UniWorks\DHCP”目录下，您可以直接运行光盘上“UniWorks\DHCP”目录下的 setup.exe，或把 UniWorks 目录下的所有文件拷贝到本地，再运行“DHCP”目录下的 setup.exe。主要安装过程与 AAA 服务器的安装过程相似，在此不再冗述。

4. 安装 Portal 服务器

安装程序在光盘的“UniWorks\PORTAL”目录下，您可以直接运行光盘上“UniWorks\PORTAL”目录下的 setup.exe，或把 UniWorks 目录下的所有文件拷贝到本地，再运行“PORTAL”目录下的 setup.exe。主要安装过程与 AAA 服务器的安装过程相似，在此不再冗述。

5. 安装管理服务器

安装程序在光盘的“UniWorks\MANAGER”目录下，您可以直接运行光盘上“UniWorks\MANAGER”目录下的 setup.exe，或把 UniWorks 目录下的所有文件拷贝到本地，再运行“MANAGER”目录下的 setup.exe。主要安装过程与 AAA 服务器的安装过程相似，在此不再冗述。

6. 安装检验

UniWorks UAS 系统安装成功后，可在 Windows 的‘开始’ －>‘程序’ 中看到 UniWorks UAS 系统程序组，包括：

- HarbourNetworks AAA Server
- HarbourNetworks DHCP Server
- HarbourNetworks Manager Server
- HarbourNetworks Portal Server



提示

用户可通过点击每个程序组中的“Uninstall”快捷方式进行各个程序组的卸载。

2.4.2 Solaris版安装

1. 安装准备

请在安装 UniWorks UAS for Solaris 版本之前，先确认计算机中安装的操作系统为 Solaris8 for SPARC 或者以上版本。如果不是，请先安装相应的操作系统之后再安装 UniWorks UAS 系统。

请确保您的系统中安装了下列软件包：

- SUNWj3dev J2SDK 1.4 development tools
- SUNWj3rt J2SDK 1.4 runtime environment
- SUNWapchr Apache Web Server (root)
- SUNWapchu Apache Web Server (usr)
- SUNWtcatu Tomcat Servlet/JSP Container
- SUNWtcatr Tomcat Servlet/JSP Container (root)
- SFWmysql mysql - MySQL Database Management System

如果您没有安装，请到 UniWorks UAS for Solaris 安装光盘中获取上述软件包。

2. 安装 AAA 服务器

第一步：获取 UniWorks UAS AAA for Solaris 软件安装包。

- 首先用超级用户 root 登录系统；
- 将 UniWorks UAS for Solaris 安装光盘放入 CDROM 中，系统将自动 mount 上光盘卷；
- 用 mount | grep cdrom 命令查看目前光盘的 mount 路径；
- 将软件安装包拷贝到工作目录下（也可以直接使用光盘中的软件包，但推荐拷贝到硬盘上）；
- 请获取光盘驱动器目录下的 UniWorksUASAAA.tar.gz 文件。

```
# ls
UniWorksUASAAA.tar.gz
#
```

第二步：软件解包

- 将软件包用 gunzip 以及 tar 命令解开：

```
# gunzip UniWorksUASAAA.tar.gz
# tar xf UniWorksUASAAA.tar
```

■ 解压后，工作目录中将出现一个 UniWorksUASAAA 目录

```
# ls
UniWorksUASAAA          UniWorksUASAAA.tar
#
```

第三步：正式安装

■ 进入刚才解压出的 UniWorksUASAAA

```
#cd UniWorksUASAAA
```

■ 执行 installer 脚本

```
# ./installer
```

将会显示如下安装信息：

```
# ./installer
*******************************************************************
 Welcome to install UniWorks UAS AAA Server(c) software!
*******************************************************************

Type CR to install UniWorks UAS AAA Server to
(/opt/HarbourNetworks/UniWorks/UAS),
 otherwise to directory you input:
```

该信息提示您输入软件安装路径，直接回车则安装到默认路径 (/opt/HarbourNetworks/UniWorks/UAS)中。

第四步：安装确认

输入正确安装路径或回车后，安装程序会出现如下提示信息，提示您在安装过程中不要使用 ctrl-c 命令终止安装，如果遇到问题，等安装后运行 uninstaller 卸载后再安装：

```
Do not use ctrl-c to interrupt 'install',it will get some problem when

 you install 'aaa' next time;wait and use 'uninstaller' to uninstall!


type 'y' to continue 'n' to exit!
```

如果安装路径已经存在，则会出现以下提示信息，提示您备份目录中的重要数据：

```
*******************************************************************
 /opt/HarbourNetworks/UniWorks/UAS/aaa already exists, MAKE SURE backup
  important data before continue install process!
*******************************************************************

Do not use ctrl-c to interrupt 'install',it will get some problem when
 you install 'aaa' next time;wait and use 'uninstaller' to uninstall!

type 'y' to continue 'n' to exit!
```

如果安装程序检测到有以前安装过的 UniWorks UAS AAA 进程正在运行，会提示您确认停止这些进程以便继续安装新版本 UniWorks UAS AAA。

如上信息所示，如果您希望继续安装，输入‘y’，否则输入‘n’中止安装。

确认继续安装后，安装程序将拷贝解压软件安装包，设置系统环境变量，创建 Mysql 数据库等，如下列信息所示：

```
type 'y' to continue 'n' to exit!
y
Checking your system and extract packages!
Set runnning ENVs,here we only set /.profile for 'sh',if your root
 shell is 'csh' or other shell, please modified your configuration
 files 'cshrc', 'ksh_profile' manually !

Install UniWorks AAA Deamon to /etc/init.d /etc/rc3.d /etc/rc0.d...

Create UniWorks AAA database...
Create database success!
```

```
Follwing services have been intalled:
 SERVICE     FORMAT
 rc.radiusd  rc.radiusd start

*********************************************************************
 Install OK, please read /opt/HarbourNetworks/UniWorks/UAS/aaa/README first!
*********************************************************************

#
```



提示

1、安装程序将只会自动更新 root 用户的 shell 环境变量配置文件。如果您要为 C Shell 或其它 Shell 设置环境变量，请手工修改相应文件。

2、如果您以前使用 Mysql 数据库，安装程序将提示您输入 Mysql 数据库 root 用户密码，并提示安装后将更改 Mysql 数据库 root 用户密码。

第五步：安装完成

UniWorks UAS AAA 服务如果要正常工作，需要运行/etc/init.d/rc.radiusd start 或重启系统。

```
# /etc/init.d/rc.radiusd start
```

3. 安装管理服务器

第一步：获取 UniWorks UAS Manage for Solaris 软件安装包

- 首先用超级用户 root 登录系统。
- 将 UniWorks UAS for Solaris 安装光盘放入 CDROM 中，系统将自动 mount 上光盘卷。
- 用 mount | grep cdrom 命令查看目前光盘的 mount 路径。
- 将软件安装包拷贝到工作目录下（也可以直接使用光盘中的软件包，但推荐拷贝到硬盘上）。
- 请获取光盘驱动器目录下的 UniWorksUASManage.tar.gz 文件。

```
# ls
```

```
UniWorksUASManage.tar.gz
#
```

第二步：软件解包

■ 将软件包用 gunzip 以及 tar 命令解开：

```
# gunzip UniWorksUASManage.tar.gz
# tar xf UniWorksUASManage.tar
```

■ 解压后，工作目录中将出现一个 UniWorksUASManage 目录

```
# ls
UniWorksUASManage          UniWorksUASManage.tar
#
```

第三步：正式安装

■ 进入刚才解压出的 UniWorksUASManage

```
#cd UniWorksUASManage
```

■ 执行 installer 脚本

```
# ./installer
```

将会显示如下安装信息：

```
# ./installer
*********************************************************************
 Welcome to install UniWorks UAS Manage Server(c) software!
*********************************************************************

Your host's IP address is '10.5.4.159'.

Checking J2SDK 1.4 runtime environment ...
```

```
Checking Tomcat Servlet/JSP Container ...

Checking Apache Web Server ...

Type CR to install UniWorks UAS Manage Server to
(/opt/HarbourNetworks/UniWorks/UAS),
 otherwise to directory you input:
```

安装程序首先检测管理服务所需的安装包（J2SDK1.4，Tomcat，Apache）之后，然后提示您输入软件安装路径，直接回车则安装到默认路径(/opt/HarbourNetworks/UniWorks/UAS)中。

第四步：安装确认

输入正确安装路径或回车后，安装程序会出现如下提示信息，提示您在安装过程中不要使用 ctrl-c 命令终止安装，如果遇到问题，等安装后运行 uninstaller 卸载后再安装：

```
Do not use ctrl-c to interrupt 'install',it will get some problem when
 you install 'manage' next time;wait and use 'uninstaller' to uninstall!

type 'y' to continue 'n' to exit!
```

如果安装路径已经存在，则会出现以下提示信息，提示您备份目录中的重要数据：

```
*********************************************************************
 /opt/HarbourNetworks/UniWorks/UAS/manage already exists, MAKE SURE backup
  important data before continue install process!
*********************************************************************

Do not use ctrl-c to interrupt 'install',it will get some problem when
 you install 'manage' next time;wait and use 'uninstaller' to uninstall!
```

```
type 'y' to continue 'n' to exit!
```

如果安装程序检测到有以前安装过的 UniWorks UAS Manage 进程正在运行，会提示您确认停止这些进程以便继续安装新版本 UniWorks UAS Manage。

如上信息所示，如果您希望继续安装输入‘y’，否则输入‘n’中止安装。

确认继续安装后，安装程序将拷贝解压软件安装包，设置系统环境变量，创建 mysql 数据库，设置 Tomcat、Apache 配置等，如下列信息所示：

```
type 'y' to continue 'n' to exit!

y


Checking your system and extract packages!



Set runnning ENVs,here we only set /.profile for 'sh',if your root
 shell is 'csh' or other shell, please modified your configuration
 files 'cshrc', 'ksh_profile' manually !



Apache and tomcat's configure files will be changed,
 old files will be backuped as '*.bk' format, such as 'httpd.conf.bk'.
Set apache and tomcat configure file ...

Create UniWorks Manage database...
Create database success!

Follwing services have been intalled:
```

```
SERVICE    FORMAT
 apache     apache restart

*********************************************************************
 Install OK, please read /opt/HarbourNetworks/UniWorks/UAS/manage/README
first!
*********************************************************************

#
```



提示

1、安装程序将只会自动更新 root 用户的 shell 环境变量配置文件。如果您要为 C Shell 或其它 Shell 设置环境变量，请手工修改相应文件。

2、如果您以前使用 mysql 数据库，安装程序将提示您输入 mysql 数据库 root 用户密码，并提示安装后将更改 mysql 数据库 root 用户密码。

3、如果您以前使用 Apache 或 Tomcat 服务，安装程序将修改 httpd.conf、 tomcat.conf、server.xml 等配置文件，原文件将被保存为 '*.bk' 形式。

第五步： 安装完成

UniWorks UAS Manage 服务如果要正常工作，需要运行/etc/init.d/apache restart 或重启系统。

```
# /etc/init.d/apache restart
```

4. 安装 Portal 服务器

第一步：获取 UniWorks UAS Portal for Solaris 软件安装包

- 首先用超级用户 root 登录系统。
- 将 UniWorks UAS for Solaris 安装光盘放入 CDROM 中，系统将自动 mount 上光盘卷。
- 用 mount | grep cdrom 命令查看目前光盘的 mount 路径。
- 将软件安装包拷贝到工作目录下（也可以直接使用光盘中的软件包，但推荐拷贝到硬盘上）。

■ 请获取光盘驱动器目录下的 UniWorksUASPortal.tar.gz 文件。

```
# ls

UniWorksUASPortal.tar.gz

#
```

第二步：软件解包

■ 将软件包用 gunzip 以及 tar 命令解开：

```
# gunzip UniWorksUASPortal.tar.gz

# tar xf UniWorksUASPortal.tar
```

■ 解压后，工作目录中将出现一个 UniWorksUASPortal 目录

```
# ls

UniWorksUASPortal          UniWorksUASPortal.tar

#
```

第三步：正式安装

■ 进入刚才解压出的 UniWorksUASPortal

```
#cd UniWorksUASPortal
```

■ 执行 installer 脚本

```
# ./installer
```

将会显示如下安装信息：

```
# ./installer

*********************************************************************

 Welcome to install UniWorks UAS Portal Server(c) software!

*********************************************************************


Your host's IP address is '10.5.4.159'.


Checking J2SDK 1.4 runtime environment ...
```

```
Checking Tomcat Servlet/JSP Container ...

Checking Apache Web Server ...

Type CR to install UniWorks UAS Portal Server to
(/opt/HarbourNetworks/UniWorks/UAS),
 otherwise to directory you input:
```

安装程序首先检测管理服务所需的安装包（J2SDK1.4，Tomcat，Apache）之后，然后提示您输入软件安装路径，直接回车则安装到默认路径(/opt/HarbourNetworks/UniWorks/UAS)中。

第四步：安装确认

输入正确安装路径或回车后，安装程序会出现如下提示信息，提示您在安装过程中不要使用 ctrl-c 命令终止安装，如果遇到问题，等安装后运行 uninstaller 卸载后再安装：

```
Do not use ctrl-c to interrupt 'install',it will get some problem when
 you install 'portal' next time;wait and use 'uninstaller' to uninstall!

type 'y' to continue 'n' to exit!
```

如果安装路径已经存在，则会出现以下提示信息，提示您备份目录中的重要数据：

```
*********************************************************************
 /opt/HarbourNetworks/UniWorks/UAS/manage already exists, MAKE SURE backup
  important data before continue install process!
*********************************************************************

Do not use ctrl-c to interrupt 'install',it will get some problem when
```

```
 you install 'manage' next time;wait and use 'uninstaller' to uninstall!

type 'y' to continue 'n' to exit!
```

如果安装程序检测到有以前安装过的 UniWorks UAS Portal 进程正在运行，会提示您确认停止这些进程以便继续安装新版本 UniWorks UAS Portal。

如上信息所示，如果您希望继续安装输入‘y’，否则输入‘n’中止安装。

确认继续安装后，安装程序将拷贝解压软件安装包，设置系统环境变量，设置 Tomcat，Apache 配置等，如下列信息所示：

```
type 'y' to continue 'n' to exit!

y

Checking your system and extract packages!

Set runnning ENVs,here we only set /.profile for 'sh',if your root
 shell is 'csh' or other shell, please modified your configuration
 files 'cshrc', 'ksh_profile' manually !

Install UniWorks Portal Deamon to /etc/init.d /etc/rc3.d /etc/rc0.d...

Apache and tomcat's configure files will be changed,
 old files will be backuped as '*.bk' format, such as 'httpd.conf.bk'.
Set apache and tomcat configure file ...

Follwing services have been intalled:
 SERVICE    FORMAT
 rc.portal    rc.portal start
```

```
 apache     apache restart


**********************************************************************

 Install OK, please read /opt/HarbourNetworks/UniWorks/UAS/portal/README
first!

**********************************************************************

#
```


提示

1、安装程序将只会自动更新 root 用户的 shell 环境变量配置文件。如果您要为 C Shell 或其它 Shell 设置环境变量，请手工修改相应文件。

2、如果您以前使用 Apache 或 Tomcat 服务，安装程序将修改 httpd.conf、tomcat.conf、 server.xml 等配置文件，原文件将被保存为 ‘*.bk’ 形式。

第五步：安装完成

UniWorks UAS Portal 服务如果要正常工作，需要运行/etc/init.d/rc.portal start 和/etc/init.d/apache restart 或重启系统。

```
# /etc/init.d/rc.portal start

# /etc/init.d/apache restart
```

5. 安装 DHCP 服务器

第一步：获取 UniWorks UAS DHCP for Solaris 软件安装包

- 首先用超级用户 root 登录系统。
- 将 UniWorks UAS for Solaris 安装光盘放入 CDROM 中，系统将自动 mount 上光盘卷。
- 用 mount | grep cdrom 命令查看目前光盘的 mount 路径。
- 将软件安装包拷贝到工作目录下（也可以直接使用光盘中的软件包，但推荐拷贝到硬盘上）。
- 请获取光盘驱动器目录下的 UniWorksUASDHCP.tar.gz 文件。

```
# ls

UniWorksUASDHCP.tar.gz
```

```
#
```

第二步：软件解包

- 将软件包用 gunzip 以及 tar 命令解开：

```
# gunzip UniWorksUASDHCP.tar.gz
# tar xf UniWorksUASDHCP.tar
```

- 解压后，工作目录中将出现一个 UniWorksUASDHCP 目录

```
# ls
UniWorksUASDHCP          UniWorksUASDHCP.tar
#
```

第三步：正式安装

- 进入刚才解压出的 UniWorksUASDHCP

```
#cd UniWorksUASDHCP
```

- 执行 installer 脚本

```
# ./installer
```

将会显示如下安装信息：

```
# ./installer
*********************************************************************
 Welcome to install UniWorks UAS DHCP Server(c) software!
*********************************************************************

Type CR to install UniWorks UAS DHCP Server to
(/opt/HarbourNetworks/UniWorks/UAS),
 otherwise to directory you input:
```

安装程序提示您输入软件安装路径，直接回车则安装到默认路径(/opt/HarbourNetworks/UniWorks/UAS)中。

第四步：安装确认

输入正确安装路径或回车后，安装程序会出现如下提示信息，提示您在安装过程中不要使用 ctrl-c 命令终止安装，如果遇到问题，等安装后运行 uninstaller 卸载后再安装：

```
Do not use ctrl-c to interrupt 'install',it will get some problem when
 you install 'dhcp' next time;wait and use 'uninstaller' to uninstall!

type 'y' to continue 'n' to exit!
```

如果安装路径已经存在，则会出现以下提示信息，提示您备份目录中的重要数据：

```
*********************************************************************
 /opt/HarbourNetworks/UniWorks/UAS/manage already exists, MAKE SURE backup
  important data before continue install process!
*********************************************************************

Do not use ctrl-c to interrupt 'install',it will get some problem when
 you install 'manage' next time;wait and use 'uninstaller' to uninstall!

type 'y' to continue 'n' to exit!
```

如果安装程序检测到有以前安装过的 UniWorks UAS DHCP 进程正在运行，会提示您确认停止这些进程以便继续安装新版本 UniWorks UAS DHCP。

如上信息所示，如果您希望继续安装输入‘y’，否则输入‘n’中止安装。

确认继续安装后，安装程序将拷贝解压软件安装包，设置系统环境变量等，如下列信息所示：

```
type 'y' to continue 'n' to exit!
y

Checking your system and extract packages!
```

```
Set runnning ENVs,here we only set /.profile for 'sh',if your root
 shell is 'csh' or other shell, please modified your configuration
 files 'cshrc', 'ksh_profile' manually !


Install UniWorks DHCP Deamon to /etc/init.d /etc/rc3.d /etc/rc0.d...

Follwing services have been intalled:
 SERVICE     FORMAT
 rc.dhcpd  rc.dhcpd start

*********************************************************************
 Install OK, please read /opt/HarbourNetworks/UniWorks/UAS/dhcp/README first!
*********************************************************************

#
```


提示

安装程序将只会自动更新 root 用户的 shell 环境变量配置文件。如果您要为 C Shell 或其它 Shell 设置环境变量，请手工修改相应文件。

第五步：安装完成

UniWorks UAS DHCP 服务如果要正常工作，需要运行/etc/init.d/rc.dhcpd start 或重启系统。

```
# /etc/init.d/rc.dhcpd start
```

6. 服务运行检验

安装完毕后，各后台服务需要通过管理服务做版权认证，然后再通过管理服务进行必要的初始化工作。

Solaris 系统下监控 UniWorks UAS 系统后台服务的方法：

（1）UniWorks UAS AAA 服务

UniWorks UAS AAA 服务依靠一个后台守护进程和一个 Mysql 后台数据库支撑：

- UniWorks UAS AAA Deamon UniWorks ：UAS AAA 后台服务
- MySQL Deamon：MySQL 数据库后台服务

判断 UniWorks UAS AAA 守护进程正常运行的方法：

```
# ps -ef  | grep radiusd

     root  2478     1  0 17:44:32 pts/3    0:01 ./radiusd -f -d ../etc/raddb
```

通过 UDP 监听端口判断 radiusd 正在运行：

```
# netstat -na |grep 1812

     *.1812                           Idle
```

判断 MySQL 正常运行的方法：

```
# ps -ef | grep mysql

   root 19674     1  0 05:19:11 pts/4    0:00 /bin/sh ./bin/safe_mysqld -O
max_connect_errors=10000 --datadir=/opt/mysql/data

  mysql 19694 19674  0 05:19:11 pts/4    0:00 /opt/mysql/bin/mysqld
--defaults-extra-file=/opt/mysql/data/my.cnf --basedir=/o

# netstat -an | grep LISTEN | grep 3306

     *.3306             *.*               0      0     0      0 LISTEN
```


注意

请不要手工修改这些服务，如果服务启动停止不正常，请和港湾网络有限公司技术支援部联系。

（2）UniWorks UAS 管理服务

UniWorks UAS 管理服务依靠 Apache＋Tomcat 后台服务和一个 Mysql 后台数据库支撑：

- Apache Deamon：Apache 后台服务
- Tomcat Deamon：Tomcat 后台服务
- MySQL Deamon：MySQL 数据库后台服务

判断 Apache 后台服务正常运行的方法：

```
# ps -ef  |grep httpd
  nobody  2473   395  0 17:43:24 ?       0:00 /usr/apache/bin/httpd
  nobody  2469   395  0 17:42:40 ?       0:00 /usr/apache/bin/httpd
  nobody  2470   395  0 17:42:40 ?       0:00 /usr/apache/bin/httpd
    root   395     1  0 15:55:12 ?       0:00 /usr/apache/bin/httpd
  nobody  2468   395  0 17:42:40 ?       0:00 /usr/apache/bin/httpd
  nobody  2467   395  0 17:42:40 ?       0:00 /usr/apache/bin/httpd
  nobody  2472   395  0 17:43:20 ?       0:00 /usr/apache/bin/httpd
    root  4076   470  0 13:26:39 pts/2    0:00 grep httpd
  nobody  2471   395  0 17:42:40 ?       0:00 /usr/apache/bin/httpd
```

判断 Tomcat 后台服务正常运行的方法：

```
# ps -ef  |grep tomcat
    root  2463     1  0 17:42:39 pts/3    0:37 /usr/j2se/bin/java -classpath
/usr/apache/tomcat/bin/bootstrap.jar:/usr/j2se/li
```

判断 MySQL 正常运行的方法：

```
# ps -ef | grep mysql
    root 19674     1  0 05:19:11 pts/4    0:00 /bin/sh ./bin/safe_mysqld -O
max_connect_errors=10000 --datadir=/opt/mysql/data
   mysql 19694 19674  0 05:19:11 pts/4    0:00 /opt/mysql/bin/mysqld
--defaults-extra-file=/opt/mysql/data/my.cnf --basedir=/o
```

```
# netstat -an | grep LISTEN | grep 3306
     *.3306              *.*              0      0     0      0 LISTEN
```



请不要手工修改这些服务，如果服务启动停止不正常，请和港湾网络有限公司技术支援部联系。

（3）UniWorks UAS Portal 服务

UniWorks UAS Portal服务依靠Apache＋Tomcat后台服务和两个后台守护进程支撑：

- UniWorks UAS Portal Deamon：UniWorks UAS Portal 后台服务
- UniWorks UAS Policy Deamon：UniWorks UAS Policy 后台服务
- Apache Deamon：Apache 后台服务
- Tomcat Deamon：Tomcat 后台服务

判断 UniWorks UAS Portal 守护进程正常运行的方法：

```
# ps -ef  |grep pscore
   root  4110    1 12 15:13:29 pts/2    0:05 ./pscore ..
```

判断 UniWorks UAS Policy 守护进程正常运行的方法：

```
# ps -ef  |grep cops
root  4107    1 28 15:13:28 pts/2    1:12 java -cp lib/cops.jar
com.harbour.cops.server.PolicyServer
```

判断 Apache 后台服务正常运行的方法：

```
# ps -ef  |grep httpd
  nobody  2473   395  0 17:43:24 ?       0:00 /usr/apache/bin/httpd
  nobody  2469   395  0 17:42:40 ?       0:00 /usr/apache/bin/httpd
  nobody  2470   395  0 17:42:40 ?       0:00 /usr/apache/bin/httpd
    root   395     1  0 15:55:12 ?       0:00 /usr/apache/bin/httpd
  nobody  2468   395  0 17:42:40 ?       0:00 /usr/apache/bin/httpd
```

```
nobody  2467   395  0 17:42:40 ?       0:00 /usr/apache/bin/httpd
nobody  2472   395  0 17:43:20 ?       0:00 /usr/apache/bin/httpd
nobody  2471   395  0 17:42:40 ?       0:00 /usr/apache/bin/httpd
```

判断 Tomcat 后台服务正常运行的方法：

```
# ps -ef  |grep tomcat
   root  2463    1  0 17:42:39 pts/3    0:37 /usr/j2se/bin/java -classpath
/usr/apache/tomcat/bin/bootstrap.jar:/usr/j2se/li
```



请不要手工修改这些服务，如果服务启动停止不正常，请和港湾网络有限公司技术支援部联系。

（4）UniWorks UAS DHCP 服务

UniWorks UAS DHCP 服务依靠一个后台守护进程支撑：

- UniWorks UAS DHCP Deamon：UniWorks UAS DHCP 后台服务

判断 UniWorks UAS DHCP 守护进程正常运行的方法：

```
# ps -ef  |grep dhcpd
root  4161    1  0 15:20:26 pts/2    0:00 ./dhcpd
```

通过 UDP 监听端口判断 dhcpd 正在运行：

```
# netstat -na  |grep *.67
              *.67                                Idle
```



请不要手工修改这些服务，如果服务启动停止不正常，请和港湾网络有限公司技术支援部联系。

3 相关知识

3.1 概述

本章对网络基本知识和 UniWorks UAS 系统所涉及的相关技术协议等进行了简要介绍。了解和掌握这些知识，将有助于您成功地使用 UniWorks UAS 系统。

3.2 网络基本知识

3.2.1 OSI（开放系统互联）参考模型

开放系统互联参考模型（OSI）是为解决不同供应商提供的设备之间的通信问题而提出的。通常情况下，不同厂家开发的网络结构和专用协议是不兼容的，为此国际标准化组织设计了 OSI 模型，将网络层次分为 7 个不同的级别，并为不同级别的数据通信建立了一套规则来解决这些兼容性问题，使来自不同厂家的设备可以互相通信。OSI 模型的层次如图 3-1 所示：

图3-1 OSI 模型的层次

7	应用层
6	表示层
5	会话层
4	传输层
3	网络层
2	数据链路层
1	物理层

在该模型中，报文起源于发送信息的计算机的应用层，然后逐步传递到物理层，再通过网络媒介传递到接收计算机的物理层，最后传递到接收机的应用层。OSI 模型各层的说明如下：

第 7 层：应用层，提供网络服务的软件，如文件传输、电子邮件、远程登录等。它在用户程序和网络之间提供接口。

第 6 层：表示层，将传出数据从机器指定的格式转换为一个国际标准格式和将传入数据从国际标准格式转换为机器指定的格式。

第 5 层：会话层，允许建立和终止一个通信路径，确保发送方是可靠的并对建立的一个连接有访问权，协调两个系统之间的通信。

第 4 层：传输层，在发送方和接收方之间提供数据流，并确保数据达到正确的目的地。该层的另一个作用是确保分组以接收方和应用程序能处理的速率发送。在接收方，传输层将分组重新组装成报文，并将其传递到更高层。

第 3 层：网络层，决定分组通过网络时采取的路径。网络层还控制网络接收分组的速率，以避免网络拥塞和能从拥塞中恢复。

第 2 层：数据链路层，提供分组传输、执行错误检测和纠错功能，以确保接收和发送分组包含相同的信息。

第 1 层：物理层，建立计算机设备和网络之间的物理连接，并提供从一个系统到其它系统的比特传输。

3.2.2 相关网络协议

1. TCP/IP（传输控制协议/网际协议）

TCP/IP 是两个使用最广泛的 Internet 协议。

TCP 提供 IP 网络上的数据传输，作用于 OSI 模型的第 4 层，能够向发送方提供到达接收方数据包的传送信息。当传送过程中出现数据包丢失情况时，TCP 可以重新发送丢失的数据包直到数据成功到达接收方或者出现网络超时。TCP 还可以识别重复信息，丢掉不需要的多余信息，使网络环境得到优化。如果发送方传送数据的速度大大快于接收方接收数据的速度，TCP 可以采用数据流控制机制减慢数据的传送速度，协调发送和接收方的数据响应。

IP 作用于 OSI 模型的第 3 层，除了可以提供网络路由之外，还具有错误控制以及网络分段等众多功能。

TCP/IP 作为一个互连设备和网络的共同起源，广泛用于连接使用不同技术的计算机。大多数管理解决方案需要 TCP/IP 作为信息源和信息载体。

2. UDP（用户数据报协议）

UDP 是一种允许一台机器上的应用程序与另外一台机器上的应用程序交换数据报而不需要确认或保证传递的协议。UDP 作用于 OSI 模型的第 4 层，即传输层。其与 TCP 的明显区别是不具备复杂的可靠性与控制机制。TCP 提供的是面向连接（即在传输前就建立好了点到点的连接）的、可靠的数据流传输，而 UDP 提供的是非面向连接（即在数据传输前不建立连接，而是在每个中间节点对数据包进行路由）的、不可靠的数据流传输。当强调传输性能而不是传输的完整性时，如音频和多媒体应用，UDP 是一个好的选择。把 SNMP 建立在 UDP 上的部分原因是设计者认为当发生网络阻塞时，UDP 较低的开销使其有更好的机会去传送管理数据；当强调数据传输的完整性、可控制性和可靠性时，则 TCP 是当然的选择。

3. HTTP 协议

HTTP 协议（Hypertext Transfer Protocol，超文本传输协议）是应用层协议，位于 OSI 模型的最上层，在该层的应用层协议还有文件传输协议 FTP、电子邮件传输协议 SMTP、域名系统服务 DNS 和网络新闻传输协议 NNTP 等。HTTP 协议用于从 WWW 服务器传输超文本到本地浏览器的传送协议。它可以使浏览器更加高效，使网络传输减少。它不仅保证计算机正确快速地传输超文本文档，还确定传输文档中的哪一部分，以及哪部分内容首先显示（如文本先于图形）等。

对于使用 UniWorks UAS 系统的 Web 用户，需要进行 Web/Portal 认证（是基于 HTTP 协议的认证方式）。

4. HTTPS 协议

HTTPS 协议是建立在 SSL （Secure Sockets Layer，安全套接字协议层）技术基础之上的 HTTP 超文本传输协议的“安全”版本。SSL 是 Netscape 公司设计的主要用于 Web 的安全传输协议，其位于 HTTP 和 TCP 协议层之间。HTTPS 和 HTTP 相比，由于存在加密和解密过程，因此，HTTPS 要比 HTTP 简单地发送未经加工的信息花费的时间要多。

3.2.3 网络硬件设备

基本的网络通信设备包括中继器、集线器、网桥、交换机、路由器。这些设备工作在 OSI 模型的不同层，使用不同的网络协议和执行不同的任务。如表 3-1 所示：

表3-1 工作在 OSI 模型不同层上的放设备

OSI 模型的层次		该层上的协议	该层上的硬件设备
7	应用层	SNMP Berkeley Services ARPA Services	网关
6	表示层		
5	会话层		
4	传输层	TCP UDP	
3	网络层	IP/IPX ICMP ARP/RARP	路由器 交换机
2	数据链路层	IEEE802.X DHCP MAC地址	网桥 交换机
1	物理层	10Base2 10Base5	简单中继器 集线器

2. 网关

网关工作在应用层，可以包含 OSI 模型的所有层。网关是一个计算系统，通过编程可以实现任何复杂的协议转换和协调，如 IP 和 IPX 之间的转换。

3. 路由器

路由器工作在网络层，其作用是连接两个使用不同技术的网络，并提供分组从一个网络传递到另一个网络的智能解决办法，还能在多个集线器和网桥之间转发流量。

4. 网桥

网桥工作在数据链路层，其作用是允许网络可以具有不同的物理信号，但又具有兼容的数据链接寻址模式。在信息从一个网段流向另一个网段时，对于不需要通过骨干网转发的信息，网桥将进行过滤，从而减少骨干局域网上的流量。网桥的通常用法是允许在一个以太局域网上的用户与一个令牌环局域网上的用户相互通信。

5. 交换机

交换机工作在数据链路层，其作用是将数据发送到目的地，该目的地由分组的低层介质访问控制（MAC）地址决定。交换机象网桥那样，对流量进行限制，且不识别网络协议。现在，新的交换设备是多层交换，或路由交换，这种设备工作在第 3

层，通过路由器智能与交换机效率的结合，从而在数据路由时可以以较高的速度进行。

6. 集线器

集线器工作在物理层。集线器只是一个多口中继器，可以用来增加整个网络的大小和在一个单一网段上的节点数量。集线器允许隔离子网错误，且能在不中断整个网络的情况下向一个网段增加节点。

7. 简单中继器

简单中继器工作在物理层，通常用于将两个网段连接成一个大段，或扩展一个已存在的网段。两个网段之间对传递的报文不进行过滤。简单中继器能对数据信号进行加强，因此可以用来扩展传送距离。简单中继器没有内置网络智能，通常严格用于信号传播。

3.3 操作系统

UniWorks UAS 系统的 V1.00 版支持多操作系统平台的应用，可运行在 Solairs、Microsoft Windows2000/XP、Linux 等多种操作系统。

有关操作系统的知识，请用户参考操作系统随带的文档资料。

3.4 NAS接入服务

随着宽带以太网建设规模的迅速扩大，为了适应用户数量急剧增加和宽带业务多样性的要求，港湾网络有限公司通过在 Hammer 系列交换机上嵌入接入服务完成用户的认证和管理功能，以便更好地支持宽带网络的计费、安全、运营和管理的要求。嵌入了接入服务的 Hammer 交换机称为网络访问服务器（Network Access Server，NAS）。

接入服务在运用 802.1x 协议和 RADIUS 协议的基础上，实现对用户接入的认证和管理功能。使用接入服务主要有以下优点：

- **简洁高效**：纯以太网技术内核，保持 IP 网络无连接特性，去除冗余昂贵的多业务网关设备，消除网络认证计费瓶颈和单点故障，易于支持多业务；

- **容易实现**：可在普通 L3、L2、IP DSLAM 上实现，网络综合造价成本低；
- **安全可靠**：在二层网络上实现用户认证，并可以通过设备实现 MAC、端口、账户和密码等绑定技术，具有很高的安全性；
- **易于运营**：控制流和业务流完全分离，易于实现多业务运营。

接入服务在运用 802.1x 基于端口的访问控制协议的基础上扩展了该协议，实现了基于用户 MAC 地址的访问控制，可以对设备一个端口上的多个接入用户分别进行认证和管理，提供对用户接入的灵活控制，同时能够与动态主机配置协议中继代理（DHCP Relay）相结合，为计费服务器提供用户的 IP 地址。

接入服务提供 3 种身份验证方式：PAP、CHAP、EAP-MD5 和 EAP-TLS 方式，根据业务运营的不同需求，可以使用其中任何一种身份验证方式实现接入服务。

3.4.1 802.1x协议

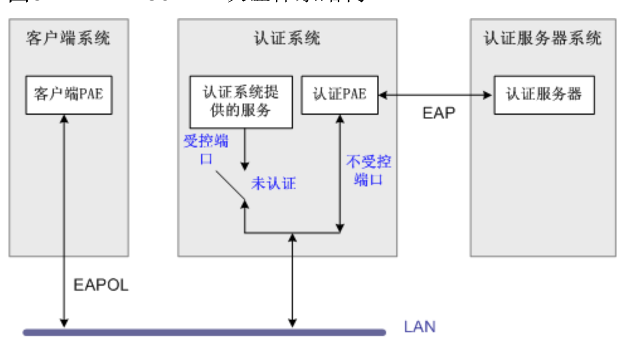
在 IEEE 802 所定义的局域网环境中，只要存在物理的连接口，未经授权的网络设备就可以直接或通过连接到局域网的设备进入局域网络。随着局域网技术的广泛应用，在很多网络环境中，往往不希望未经授权的设备或用户连接到网络，使用网络提供的资源和服务。特别是在运营网络中的应用，对其安全认证的要求已经提到了议事日程上。如何既能够利用局域网技术简单、廉价的组网特点，同时又能够对用户或设备访问网络的合法性提供认证，是目前业界讨论的焦点。IEEE 802.1x 协议正是在这样的背景下提出的。

IEEE 802.1x 称为基于端口的访问控制协议（Port Based Network Access Control Protocol），该协议在利用 IEEE 802 LAN 的优势基础上提供了对连接到局域网的设备或用户进行认证和授权的一种手段。通过此方式的认证，能够在 LAN 这种多点访问环境中提供一种点对点识别用户的方式。这里的端口是指连接到 LAN 的一个单点结构，可以是被认证系统的 MAC 地址，也可以是服务器或网络设备上连接 LAN 的物理端口，或者是在 IEEE 802.11 无线 LAN 环境中定义的工作站和访问点。

1. 802.1x 体系结构

IEEE 802.1x 协议的体系结构包括三个重要的组成部分：Supplicant 客户端、Authenticator System 认证系统、Authentication Server 认证服务器。下图描述了三者之间的关系以及相互之间的通信。

图3-2 IEEE 802.1x 认证体系结构



客户端系统一般指用户终端系统，该终端系统通常需要安装一个客户端软件，用户通过启动这个客户端软件发起 802.1x 协议的认证过程。为了支持基于端口的接入控制，客户端系统需支持 EAPOL（Extensible Authentication Protocol Over LAN）协议。

认证系统通常指那些支持 802.1x 协议的网络设备，如港湾网络有限公司的 Hammer 系列交换机和无线访问点设备。支持 802.1x 协议的网络设备对应不同的业务端口（可以是物理端口，也可以是用户设备的 MAC 地址）有两个逻辑端口：受控端口（Controlled Port）和不受控端口（Uncontrolled Port）。不受控端口始终处于双向连通状态，主要用来传递 EAPOL 协议帧，可保证客户端始终能够发出或接受认证。受控端口只有在认证通过的状态下才可打开，用于传递网络资源和服务。受控端口可配置为双向受控、仅输入受控两种方式，以适应不同的应用环境。如果用户未通过认证，则受控端口处于未认证状态，用户无法访问认证系统提供的服务。图 3-2 中认证系统的受控端口处于未认证状态，因此客户端无法访问认证系统提供的服务。

PAE 是端口访问实体（Port Access Entity），分为客户端 PAE 和认证系统 PAE：

- 客户端 PAE：位于客户端，主要负责响应来自认证系统建立信任关系的请求。
- 认证系统 PAE：位于认证系统，负责与客户端的通信，把从客户端收到的信息传送给认证服务器以完成认证。

认证系统的 PAE 通过不受控端口与客户端 PAE 进行通信，二者之间运行 EAPOL 协议。认证系统的 PAE 与认证服务器之间运行 RADIUS（Remote Authentication Dial In User Service）协议。

认证系统和认证服务器之间的通信可以通过网络进行，也可以使用其他的通信通道。例如当认证系统和认证服务器集成在一起时，两个实体之间的通信就可以不采用 RADIUS 协议。

认证服务器通常为 RADIUS 服务器，该服务器可以存储有关用户的信息，比如用户所属的 VLAN、CAR 参数、优先级、用户的访问控制列表等等。当用户通过认证后，认证服务器会把用户的相关信息传递给认证系统，由认证系统构建动态的访问控制列表，用户的后续流量将接受上述参数的监管。

图 3-2 描述了终端用户的认证机制，对于网络设备之间的认证也是一样。例如：当一个网络设备 A 要求访问网络设备 B 所提供的服务时，系统 A 的 PAE 就成为客户端（Suppliant），系统 B 的 PAE 为认证系统（Authenticator）；如果 B 要求访问 A 所提供的服务时，B 的 PAE 就成为客户端，A 的 PAE 就成为认证系统。

2. 802.1x 认证机制

802.1x 作为一种认证协议，在实现的过程中有很多重要的工作机制，这里主要介绍其中四种的机制：

- 认证发起机制
- 退出认证机制
- 重新认证机制
- 认证报文丢失重传机制

(1) 认证发起机制

认证过程可以由用户主动发起，也可以由认证系统发起。一方面当认证系统探测到有未经过认证的用户使用网络时，就会主动发起认证,另一方面客户端可以通过客户端软件向认证系统发送 EAPOL-Start 报文发起认证。

◎ 由认证系统发起的认证

当认证系统检测到有未经认证的用户使用网络时，就会发起认证。在认证开始之前，端口的状态被强制“未认证”。

如果客户端的身份标识不可知，则认证系统会发送 EAP-Request/Identity 报文，请求客户端发送身份标识。这样，就开始了典型的认证过程。

客户端在收到来自认证系统的 EAP-Request/Identity 报文后，将发送 EAP-Response/Identity 报文响应认证系统的请求。

认证系统支持定期的重新认证，可以随时对一个端口发起重新认证的过程。如果端口状态为已认证状态，则当认证系统发起重新认证时，该端口通过认证，状态保持不变；如果未通过认证，则端口的状态改变为未认证状态。

◎ 由客户端发起认证

如果用户要上网，则可以通过客户端软件向认证系统发送 EAPOL-Start 报文主动发起认证。认证系统在收到客户端发送的 EAPOL-Start 报文后，会发送 EAP-Request/Identity 报文响应用户请求，要求用户发送身份标识，这样就启动了一个认证过程。

(2) 退出认证机制

有以下几种方式可以造成认证系统把端口状态从已认证状态改变成未认证状态：

a) 客户端未通过认证服务器的认证；
b) 管理性的控制端口始终处于未认证状态；
c) 与端口对应的 MAC 地址出现故障（管理性禁止或硬件故障）；
d) 客户端与认证系统之间的连接失败，造成认证超时；
e) 重新认证超时；
f) 客户端未响应认证系统发起的认证请求；
g) 客户端发送 EAPOL-Logoff 报文，主动下线。

退出已认证状态的直接结果就是导致用户下线，如果用户要继续使用网络则要重新发起一个认证过程。为什么要专门提供一个 EAPOL-Logoff 机制呢？主要是出于如下的安全考虑：当一个用户从一台终端退出后，很可能其他用户不通过发起一个新的认证过程，就可以利用该设备访问网络。提供专门的退出机制，以确保用户与认证系统专有的会话进程被中止，可以防止用户的访问权限被他人盗用。通过发送 EAPOL-Logoff 报文，可以使认证系统将对应的端口状态改变为未认证状态。

(3) 重新认证机制

为了保证用户和认证系统之间的链路处于激活状态，而不因为用户端设备发生故障造成异常死机，从而影响对用户计费的准确性，认证系统可以定期发起重新认证过程，该过程对于用户是透明的，即用户无需再次输入用户名和密码。

重新认证由认证系统发起，时间是从最近一次成功认证后算起。交换机上的重新认证功能可以激活或关闭，默认情况下是关闭的。重新认证的时间间隔默认值为 3600 秒（一个小时）。


注意

重新认证的时间设定需要认真的规划，认证系统对端口进入的 MAC 地址的检测能力会影响到该时间的设定。如果对 MAC 地址的检测比较可靠，则重新认证时间可以设长一些。

(4) 认证报文丢失重传机制

对于认证系统和客户端之间通信的 EAP 报文，如果发生丢失，由认证系统负责进行报文的重传。在设定重传的时间时，考虑网络的实际环境，通常会认为认证系统和客户端之间报文丢失的几率比较低以及传送延迟低，因此一般通过一个超时计数器来设定，默认重传时间为 30 秒钟。

由于对用户身份合法性的认证最终由认证服务器执行，认证系统和认证服务器之间的报文丢失重传也很重要。

另外注意，对于用户的认证，在执行 802.1x 认证时，只有认证通过后，才能由 DHCP 发起（如果配置为 DHCP 的自动获取）和 IP 地址分配的过程。当客户终端配置了 DHCP 自动获取 IP 地址时，则可能在未启动 802.1x 客户端之前，就发起了 DHCP 的请求，而此时认证系统处于禁止通行状态，这样认证系统会丢掉 DHCP 请求帧。

3. 协议实现内容

802.1x 协议在实现整个安全认证的过程中，其三个关键部分（客户端、认证系统、认证服务器）之间是通过不同的通信协议进行交互的，因此有必要对其相关的通信协议做一介绍。

EAP 协议

802.1x 协议采用 EAP 协议在客户端、认证系统和认证服务器之间进行通信。EAP（Extensible Authentication Protocol 扩展的认证协议，RFC 2284）是 PPP 认证的一个通用协议，支持多种认证机制。EAP 在链路控制（LCP）阶段并不选择好一种认证机制，而是把这一步推迟到认证阶段，这就允许认证系统在确定某种特定认证机制之前请求更多的信息。

通过支持 EAP 协议，认证系统只需控制其受控端口的状态，而并不干涉通过非受控端口在客户端和认证服务器之间传递的认证信息，这样可实现认证流和业务流的完全分离。可以使用认证服务器来实现各种认证机制，认证系统仅仅需要传送认证信息，并根据认证返回的结果控制受控端口的状态。

EAP 帧结构如图 3-3 所示：

图3-3 EAP 帧结构

Octet Number	
Code	1
Identifier	2
Length	3-4
Data	5-N

EAP 帧格式中各字段含义如下：

字段	占用字节数	描述
Code	1个字节	表示EAP帧的四种类型： 1．Request 2．Response 3．Success 4．Failure
Identifier	1个字节	用于匹配Request和Response。Identifier的值和系统端口一起单独标识一个认证过程
Length	2个字节	表示EAP帧的总长度
Data	0或更多字节	表示EAP数据

EAPOL 协议

802.1x 协议定义了一种报文封装格式，这种报文称为 EAPOL（EAP over LANs 局域网上的扩展认证协议）报文，主要用于在客户端和认证系统之间传送 EAP 协议报文，以允许 EAP 协议报文在 LAN 上传送。

EAPOL 帧结构如图 3-4 所示：

图3-4 EAPOL 帧结构

	Octet Number
PAE Ethernet Type	1-2
Protocol Version	3
Packet Type	4
Packet Body Length	5-6
Packet Body	7-N

EAPOL 帧格式中各字段含义如下：

字段	占用字节数	描述
PAE Ethernet Type	2个字节	表示协议类型，802.1x分配的协议类型为888E
Protocol Version	1个字节	表示EAPOL 帧的发送方所支持的协议版本号。本规范使用值为0000 0001
Packet Type	1个字节	表示传送的帧类型，如下几种帧类型： a) EAP-Packet. 值为 0000 0000 ，表示为EAP帧 b) EAPOL-Start.值为0000 0001 ， 表示为EAPOL-Start 帧 c) EAPOL-Logoff. 值为0000 0010，表示为EAPOL-Logoff请求帧 d) EAPOL-Key.值为0000 0011 ， 表示为EAPOL-Key 帧. e) EAPOL-Encapsulated-ASF-Alert. 值为0000 0100
Packet Body Length	2个字节	表示Packet Body的长度
Packet Body	0或更多字节	如果Packet Type为EAP-Packet、EAPOL-Key或EAPOL-Encapsulated-ASF-Alert的值，则Packet Body取相应的值；对于其他帧类型，该值为空。

EAPOL 帧可以携带 802.1q 的 VLAN 标记。

EAPOL 帧在二层传送时，必须要有目标 MAC 地址，当客户端和认证系统彼此之间不知道发送的目标时，其目标 MAC 地址使用由 802.1x 协议分配的组播地址 01-80-c2-00-00-03。

4. 与不支持 802.1x 的设备的兼容

对于从一个没有认证的系统过渡到认证系统，最理想的状态是希望能够平滑的进行过渡。由于 802.1x 协议是一个比较新的协议，如果应用在原有的旧网络中，则可能存在与不支持 802.1x 协议的设备的兼容性问题。

如果客户端支持 802.1x 协议，而网络设备不支持（也就是没有认证系统），则客户端是不会收到认证系统响应的 EAP-Request/Identity 报文。在 802.1x 认证发起阶段，客户端首先发送 EAPOL-Start 报文到 802.1x 协议组申请的组播 MAC 地址，以查询网络上可以处理 802.1x 的设备（即认证系统），由于网络中没有设备充当认证系统，所以客户端是得不到响应的。因此客户端在发起多次连接请求无响应后，自动认为已经通过认证。

如果客户端不支持 802.1x 协议，而网络中存在 802.1x 协议的认证系统，则客户端是不会响应认证系统发送的 EAP-Request/Identity 报文，因此端口会始终处于未认证状态。在这种情况下，客户端只能根据协议参数 OperControlledDirections 设定的值通过受控端口访问认证系统，通过未受控端口访问某些通过设置可以访问的服务。

3.4.2 RADIUS协议

RADIUS 的全称为（Remote Access Dail-In User Service），它是对远程拨号用户访问进行认证的一种协议，是在 RADIUS Server 和 RADIUS Client 之间进行认证、授权、计费的协议标准。认证即辨别用户是谁的过程，通常该过程通过输入有效的用户名和密码实现；授权是指对完成认证过程的用户授予相应权限，解决他能做什么的问题，在一些身份认证的实现中，认证和授权是统一在一起的；计费（Accounting）则是统计用户做过什么的过程，包括用户使用的时间和费用，可通过用户占用系统的时间、接收和发送的信息量来衡量。

RADIUS 采用 Client/Server 模型，在 NAS 上运行的是 Client 端，负责将用户信息传送到指定的 RADIUS 服务器上，并根据服务器返回的结果进行相应的处理。RADIUS 服务器包括两种类型：授权认证服务器和计费服务器。授权认证服务器（RADIUS Authentication Server）负责接收用户的连接请求、验证用户身份，并返回给客户需要的相关配置信息。一个授权认证服务器也可以作为 RADIUS 客户的代理，将其连接到另一个授权认证服务器。计费服务器（RADIUS Accounting Server）负责接受用户计费开始请求和计费结束请求，并实现计费功能。

RADIUS 具有以下属性：

- RADIUS 以 Client/Server 模式工作，实现了对远程用户的身份认证、授权和计费功能。
- RADIUS Client 主要用来将用户信息传递给 RADIUS Server；Server 则对用户进行认证，并返回用户的配置信息。
- 为保证传输的安全性，RADIUS 报文携带由 MD5 算法求得的 128 位验证字。
- 认证具有灵活性。采取多种认证机制，包括 PAP 和 CHAP。

3.5 PPPoE协议

PPPoE（PPP over Ethernet，以太网上点对点协议）是在以太网中传输 PPP 帧信息的技术。它通过把最经济的局域网技术以太网和点对点协议的可扩展性及管理控制功能结合在一起，使网络服务提供商或运营商能够利用可靠和熟悉的技术来加速部署高速互联网业务。它使服务提供商在通过数字用户线、电缆、调制解调器或无线连接等方式，提供支持多用户的宽带接入服务时更加简便易行。同时该技术亦简化了最终用户动态选择这些服务时的操作。

PPPoE 协议共包括两个阶段：发现阶段（PPPoE Discovery Stage）和会话阶段（PPPoE Session Stage）。当一主机希望能够开始一个 PPPoE 会话时，它首先会在广播式的网络上寻找一个宽带接入服务器，当然可能网络上会存在多个宽带接入服务器，对于主机而言则会根据各宽带接入服务器所能提供的服务或用户的预先的一些配置来进行相应的选择。当主机选择完了所需要的宽带接入服务器后，就开始和宽带接入服务器建立一个 PPPoE 会话进程。在这个过程中宽带接入服务器会为每一个 PPPoE 会话分配一个唯一的进程 ID，会话建立起来后就开始了 PPPoE 的会话阶段，在这个阶段中已建立好点对点连接的双方（这种点对点的结构与 PPP 不一样，它是一种逻辑上的点对点关系）就采用 PPP 协议来交换数据报文，从而完成一系列 PPP 的过程，最终将在这点对点的逻辑通道上进行网络层数据报的传送。

PPPoE 协议具有以下优点：

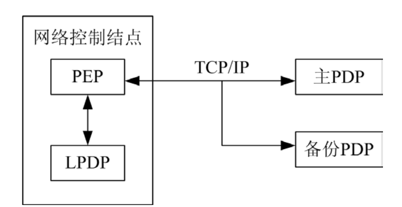
- 安装与操作方式类似于以往的拨号网络模式，方便用户使用；
- 用户处的 xDSL 调制解调器无须任何配置；
- 允许多个用户共享一个高速数据接入链路。适应小型企业和远程办公的要求；
- 终端用户可同时接入多个 ISP，这种动态服务选择的功能可以使 ISP 容易创建和提供新的业务；
- 兼容目前所有的 xDSL Modem 和 DSLAM；

- 可与 ISP 现有接入结构相融合。

3.6 COPS协议

COPS（Common Open Policy Service，公共开放策略服务）协议是基于 C/S 模式的客户端策略控制协议。COPS 协议提供了在策略服务器（PDP or Policy Decision Point）和策略客户端（PEP or Policy Enforcement Points）之间传输、管理和控制策略信息的通用方法。COPS 协议提供了在异构网络环境下实现一致的策略控制信息管理和维护方法。如图 3-5 所示：

图3-5 COPS 协议策略控制信息管理和维护



COPS 协议使用 TCP 协议在 PDP 和 PEP 之间交换协议报文。正常情况下 PEP 从主 PDP 服务器获取策略控制信息。当 PEP 到主 PDP 服务器的网络连接发生故障的时候，则 PEP 向备份 PDP 服务器发送策略配置请求。如果 PEP 到主备 PDP 服务器的网络连接都发生了故障，那么 PEP 由本地 LPDP 处理策略配置请求。

PEP 在逻辑上分为多个客户端类型。不同的客户端类型可以从相同的主备 PDP 服务器获取策略配置信息，也可以从不同的主备 PDP 服务器获取不同客户端类型的策略控制信息。

UniWorks UAS 的 Portal 服务器中包含一个实现了 COPS 协议的策略服务器，即从 COPS 协议上考虑 Portal 服务器就是一个 PDP。Portal 服务器当与实现了 COPS 协议的 PEP（港湾网络有限公司的 PowerHammer ESR 系列路由器已经实现了该协议）一起部署应用时，可以实现对认证用户的策略化管理，如用户的 ACL、QoS 等。

策略服务器的配置包括：对 NAS 中 COPS 部分进行配置（请参见港湾网络有限公司 PowerHammer ESR 系列路由器软件配置手册）和策略服务器的配置。这两项配置没有先后关系。只有 COPS 的相关参数配置正确，策略服务器才能够正常工作。

3.7 QoS

QoS（Quality of Service）指 IP 的服务质量，是指 IP 数据流通过网络时的性能。它的目的就是向用户的业务提供端到端的服务质量保证。它有一套度量指标，包括业务可用性、延迟、可变延迟、吞吐量和丢包率。QoS 在可预测、可测量性方面比传统 IP 有了很大提高，基本解决了商业用户的需求，因而势必可以吸引更多的商业用户，形成一个新的利润增长点，带来可增值的业务种类。另外， QoS 还带来了更高效的带宽使用率等。因此可以说 QoS 将是今后一段时间促进 IP 网络增长的关键技术。

不同的应用有不同的 QoS 需求，如语音、图像对抖动和时延敏感，则要求带宽保证和高的优先级；数据和文件传输则对时延不敏感，则可在保证带宽的前提下采用较低的优先级。

3.8 ACL

ACL 及 access-list，主要为访问控制提供包过滤条件，另外也为带宽管理、入侵检测、应用代理等提供过滤规则，找出满足条件的数据包。

ACL 相当于过滤规则，找出满足条件的数据包，ACL 的 listid 主要分为一下几类：

- <1-99>：标准 ACL，只能使用源 IP 进行过滤；
- <100-199>：扩展 ACL，提供基于源 IP 和目标 IP 的过滤；
- <1300-1999>：标准 ACL，提供基于源 IP 和以及源端口的过滤；
- <2000-2699>：扩展 ACL，提供基于源地址、目标地址、源端口和目标端口的过滤；
- <2700-2999>：扩展 ACL，提供基于源地址、目标地址、TCP、UDP 端口的过滤。

4 系统启动

4.1 概述

UniWorks UAS 系统启动包括后台服务启动和管理服务器启动两部分。管理员必须确定后台服务正在运行后，才能启动 UniWorks UAS 系统的管理服务器。

4.2 启动后台服务

4.2.1 Windows版

系统后台服务包括：

- **Harbour AAA Service**：是安装 AAA 服务器后注册的后台服务，实现对用户的认证、授权和计费功能；
- **Harbour DHCP Service**：是安装 DHCP 服务器后注册的后台服务，与 Harbour AAA Service 配合完成统一地址分配功能；
- **Harbour Portal Service 和 Harbour Policy Service**：是安装 Portal 服务器后注册的后台服务，实现 Web 认证、用户 ACL 策略下发、内容服务计费以及灵活的业务拓展功能；
- **MySql 或 Oracle 等数据库服务**：安装 AAA 服务器后注册的后台服务，实现用户认证数据及计费数据支持。
- **Apache2**：安装 Portal 服务器或者管理服务器后注册的后台服务，实现 Portal Web 服务或管理 Web 服务的支持。

后台服务在 UniWorks UAS 系统安装完成后，由后台程序自动在操作系统中注册，并在机器重启后自动启动。而且在每次启动 Windows 时会自动加载该服务，用户不需要手工启动后台服务。

当然，本系统的后台服务也和系统的其它服务一样，用户可以在 Windows 系统的‘开始’ －＞‘设置’中，或‘我的电脑’中选择‘控制面板’，通过‘管理工具’

－＞‘服务’快捷键启动 Windows 系统的服务面板。在服务面板中可以找到 UniWorks UAS 系统的后台服务名称，用户可以根据需要查看并修改 UniWorks UAS 系统后台服务的运行状态、启动类型等属性。

4.2.2 Solaris版

参见 2.4.2 节的相关内容。

4.2.3 AAA服务

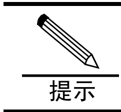
1. 功能：

AAA 服务是安装 AAA 服务器后注册的后台服务，是 UniWorks UAS 系统的核心，实现对用户的认证、授权和计费功能。具体内容包括：

- 支持标准 RADIUS 认证协议，其中认证方式包括：CHAP、PAP、EAP-MD5 和 EAP-TLS；
- 支持标准 RADIUS 计费协议，并支持港湾网络有限公司接入设备的实时计费服务；
- 支持标准 RADIUS 属性及港湾网络有限公司自定义属性的管理；
- 支持港湾网络有限公司 CUT 报文，并能灵活触发和管理；
- 地址分配功能，通过本地地址池或与 DHCP 服务组件配合两种方式；
- 结合港湾网络有限公司自定义属性，支持基于用户 MAC、IP、VLAN 和 PORT 等的绑定认证，并支持基于用户或组的 ACL、上下行带宽管理以及用户的端口反查功能；
- 对原始的计费信息进行数据库存储，并可根据实时计费报文，进行实时更新。支持对用户上下线时间、流入流出流量(目前只有 FlexHammer 系列的接入设备支持)的记录，提供对原始计费信息查询的接口，导出方式(导出到文件)认证计费标准协议的支持。

2. 特点：

- 与 DHCP 服务器配合完成统一地址分配功能
- 与港湾网络有限公司的 PowerHammer ESR 系列路由器配合实现实时 CUT、端口反查等特色功能



DHCP服务器可以看作是AAA服务器的一个组件，与AAA服务器配合完成统一地址分配功能。

4.2.4 DHCP服务

DHCP 服务是安装 DHCP 服务器后注册的后台服务，与 AAA 服务配合完成统一地址分配功能。

4.2.5 Portal和Policy服务

1. 功能：

Portal 和 Policy 服务是安装 Portal 服务器后注册的后台服务，实现 Web 认证、用户 ACL 策略下发、内容服务计费以及灵活的业务拓展功能（服务选择及内容定制等功能在 V1.00 版本未实现）。具体内容包括：

- Web 方式用户接入，使用标准 Web 浏览器作为客户端实现用户认证上网功能；
- 用户状态实时服务，认证通过后在浏览器小窗口中提示用户在线状态等信息，同时提供下线操作接口；
- 强制 Portal 重定向功能，与港湾网络有限公司的 PowerHammer ESR 系列路由器配合完成此项功能；
- 用户 ACL 策略下发功能，通过 COPS 协议将预先在数据库中配置的策略下发给 PowerHammer ESR 系列路由器。

2. 特点：

- 内置 COPS 服务器实现强大的用户策略的配置
- HTTPS 安全 Web 认证

4.3 启动管理服务器

管理服务器使用 Web 方式对 AAA 服务器、DHCP 服务器和 Portal 服务器进行统一的监控和配置。具体内容包括：

- 提供安全、可靠的管理人机接口，为系统管理员或远程管理用户监控、配置服

务器和进行日志管理提供方便、直观的操作管理界面。

- 提供详实的服务器运行状态信息；
- 将系统管理员的管理操作转化为管理消息发送给各个服务器，并把各服务器的响应结果反馈给系统管理员，从而对分布式结构的各个后台服务器实现统一方便的管理。

管理服务器特点：

- 由于 RADIUS、DHCP 和 Portal 服务器可能分布于网络的不同主机上，所以系统为分布式结构。
- 多种手段实现安全管理：

(1) 为了防止恶意主机对服务器的连接，各个服务器需要对允许建立连接的主机 IP 范围进行限制，将其保存在配置文件中。当监听到客户端的连接请求时将客户端 IP 与配置文件中的规定范围进行比较，拒绝不信任的 IP 所发送的连接请求。

(2) 为了防止恶意盗用可信任主机的 IP 对服务器发送管理命令，管理服务器和各个服务器需要保存一个他们所共享的密钥。管理服务器在发送消息和接受数据包的时候根据共享密钥对数据包进行校验，校验通过则响应管理服务器的命令请求，否则将数据包丢弃。

(3) 为了限制客户端对管理服务器的连接，在客户端登录到管理服务器的时候需要进行用户验证。用户分为超级用户和普通管理员，不同用户的权限管理分目录实现。

管理服务器启动：

- Windows 版：选择“开始”－＞“程序” －＞“HarbourNetworks Manage server” －＞“Management Server Page”；
- Solaris 版：运行以下命令或者在系统重启时自动运行管理服务

```
# /etc/init.d/apache restart
```

4.3.2 登录

管理服务器启动后，首先会要求用户进行身份验证。用户需输入正确的用户名和密码，然后，点击‘登录’按钮才能进入系统。

UniWorks UAS 系统提供了一个预置用户：

- 用户名：supervisor，口令：harbour

您可以在登录后修改密码，以保证系统安全。具体方法请参见第 10 章“安全管理”

的相关内容。

4.3.3 首页

输入正确的用户名和密码后，用户即可进入系统，进行服务器的管理配置和用户管理等。

系统刚安装时，在管理服务器管理页面上方的菜单中仅有‘安全管理’和‘退出’选项。

管理员在首页中须先对 AAA 服务器、Portal 服务器、DHCP 服务器以及用户管理服务器进行地址添加操作（详见第 5 章的相关内容）。



提示

欲使用管理服务器对 AAA 服务器、DHCP 服务器和 Portal 服务器进行监控和管理，须先添加相应的服务器地址。添加某类型的服务器地址成功后，首页页面上方将显示进入该服务器管理的链接图标，点击图标便可进入该服务器的管理页面。

5 服务器配置

5.1 概述

UniWorks UAS 系统支持 AAA 服务器、DHCP 服务器和 Portal 服务器的主备倒换，以提高系统的可靠性；支持 AAA 服务器、DHCP 服务器、Portal 服务器与管理服务器之间的共享密钥管理，以提高系统管理的安全性。

管理员要对 AAA 服务器、DHCP 服务器和 Portal 服务器进行可靠、安全的监控和管理，须在成功登录并进入系统后，先配置 AAA 服务器、Portal 服务器、DHCP 服务器和管理服务器的地址、共享密钥。

5.2 AAA服务器配置

5.2.1 配置主服务器地址

在管理服务器首页‘AAA 管理’的‘主服务器地址’栏中输入欲管理的 AAA 服务器的 IP 地址。点击‘添加’按钮后，出现新添加的服务器配置结果如图 5-1 所示：

图5-1 AAA 服务器配置结果

服务器类型	IP地址	共享密钥	
AAA服务器	10.5.4.195	harbour_networks	修改密钥

返 回

为了实现安全管理，服务器与管理服务器之间需配置共享密钥。共享密钥的默认值为‘harbour_networks’。为简化管理员操作，在添加服务器地址后，系统会自动将该服务器的共享密钥设为默认值。点击‘返回’ 按钮，回到首页。

共享密钥可以修改。点击‘修改密钥’，出现页面如图 5-2 所示：

图5-2 修改密钥

更改管理服务器与 AAA服务器 （ 10.5.4.195 ）的共享密钥	
新密钥	
确认密钥	

确定

修改密钥后，点击页面上方的‘首页’选项回到首页，继续进行服务器地址的添加、修改或删除配置。



提示

管理员可以对 AAA 主服务器进行删除。删除 AAA 主服务器后，AAA 服务器选项将从首页上部菜单中消失。

5.2.2 配置备服务器地址

为了提高系统运行的可靠性，管理员需给系统配置备服务器，本系统支持服务器的主备倒换。

备服务器的地址配置和密钥管理操作与主服务器相同，在此不再冗述。



提示

在有备服务器的情况下，管理员删除 AAA 主服务器后，备服务器将自动转为主服务器。

5.3 Portal服务器配置

5.3.1 配置主服务器地址

在管理服务器首页‘Portal 管理’的‘主服务器地址’栏中输入欲管理的 Portal 服务器的 IP 地址。点击‘添加’ 按钮后，管理服务器在添加 Portal 服务器的同时，自动添加 Policy 服务器。Policy 服务器的 IP 地址与 Portal 服务器的地址相同。出现新添加的服务器配置结果如图 5-3 所示：

图5-3 Portal 服务器配置结果

服务器类型	IP地址	共享密钥	
Portal服务器	10.5.4.17	harbour_networks	修改密钥
Policy服务器	10.5.4.17	harbour_networks	修改密钥

返 回

点击‘修改密钥’，可对 Portal 服务器或 Policy 服务器与管理服务器之间的共享密钥进行修改。

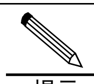

提示

管理员可以对 Portal 主服务器进行删除。删除 Portal 主服务器后，Portal 服务器选项将从首页上部菜单中消失。

5.3.2 配置备服务器地址

为了提高系统运行的可靠性，管理员需给系统配置备服务器，本系统支持服务器的主备倒换。

备服务器的地址配置和密钥管理操作与主服务器相同，在此不再冗述。


提示

在有备服务器的情况下，管理员删除 Portal 主服务器后，备服务器将自动转为主服务器。

5.4 DHCP服务器配置

5.4.1 配置主服务器地址

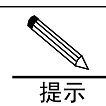
在管理服务器首页‘DHCP 管理’的‘主服务器地址’栏中输入欲管理的 DHCP 服务器的 IP 地址。点击‘添加’后，出现新添加的服务器配置结果如图 5-4 所示：

图5-4 DHCP 服务器配置结果

服务器类型	IP地址	共享密钥	
DHCP服务器	10.5.4.195	harbour_networks	修改密钥

返 回

点击‘修改密钥’，可对 DHCP 服务器与管理服务器之间的共享密钥进行修改。


提示

管理员可以对 DHCP 主服务器进行删除。删除 DHCP 主服务器后，DHCP 服务器选项将从首页上部菜单中消失。

5.4.2 配置备服务器地址

为了提高系统运行的可靠性，管理员需给系统配置备服务器，本系统支持服务器的主备倒换。

备服务器的地址配置和密钥管理操作与主服务器相同，在此不再冗述。


提示

在有备服务器的情况下，管理员删除 DHCP 主服务器后，备服务器将自动转为主服务器。

5.5 管理服务器配置

在管理服务器首页‘用户管理’中的管理服务器配置选项如图 5-5 所示：

图5-5 管理服务器配置

服务器地址	10.5.4.195		
用户名	root		
密码	**************	修 改	删 除
确认密码	**************	读取AAA配置	

此处请输入已经配置好的具有足够权限的数据库管理员用户名及密码。

为了方便管理员操作，UniWorks UAS 系统支持从当前 AAA 服务器配置中直接读

取管理服务器配置。在 AAA 服务器已配置的前提下，点击“读取 AAA 配置”按钮，服务器地址、用户名和密码等配置信息将直接导入管理服务器的配置项。点击‘修改’按钮，用户可对管理服务器配置进行修改。


提示

点击‘删除’按钮，用户管理服务器选项将从首页上方的菜单中消失。



AAA 服务器管理

6.1 概述

AAA 是 Authentication，Authorization and Accounting（认证、授权和计费）的简称。AAA 服务器是港湾网络有限公司推出的 UniWorks UAS 系统的核心部分，是基于标准 RADIUS 协议的认证、授权、计费管理服务器。该服务器灵活支持 PAP、CHAP、EAP-MD5 和 EAP-TLS 等多种认证方式，并拥有安全的绑定功能，对数据的存储提供安全保障；支持实时计费功能及多种后台数据库，并提供数据迁移功能；AAA 服务器的授权主要是指访问控制，包括：

- 哪些用户可以通过我们的接入设备访问网络？
- 具有访问权限的用户可以得到哪些服务？

AAA 授权主要是通过本地验证来确定哪些用户可以被授权使用哪些服务，对用户进行访问控制，使不同的登录用户具有不同的使用级别。

6.1.1 身份验证方式

AAA 服务提供四种身份验证方式：PAP、CHAP、EAP-MD5 和 EAP-TLS 方式。根据业务运营的不同需求，可以使用其中任何一种身份验证方式实现接入服务：

- 使用 PAP 方式进行身份验证：NAS 或 Portal 服务器在接收到用户上线请求的信息后，发送 RADIUS ACCESS REQUEST/PAP 报文到 RADIUS 服务器，RADIUS 服务器对用户进行认证，返回 RADIUS ACCESS ACCEPT（如果认证通过）报文到 NAS 或 Portal，NAS 或 Portal 完成相应操作允许用户接入。

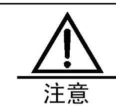
- 使用 CHAP 方式进行身份验证：NAS 或 Portal 服务器在接收到用户上线请求的信息后，发送 RADIUS ACCESS REQUEST/CHAP 报文到 RADIUS 服务器，RADIUS 服务器对用户进行认证，返回 RADIUS ACCESS ACCEPT（如果认证通过）报文到 NAS 或 Portal，NAS 或 Portal 完成相应操作允许用户接入。

- 使用 EAP-MD5 方式进行身份验证：NAS 在接收到用户上线请求的信息后，发送 ACCESS-REQUEST 到 RADIUS 服务器，RADIUS 服务器生成 challenge 信息，并发送 ACCESS-CHALLENGE 报文到 NAS；NAS 发送 EAP-REQUEST/CHALLENGE 报文到用户终端，用户终端发送 EAP-RESPONSE/MD5-CHALLENGE 报文到 NAS；NAS 将从用户终端收到 EAP-RESPONSE/MD5-CHALLENGE 报文封装到 RADIUS ACCESS REQUEST 报文中，并发送到 RADIUS 服务器，RADIUS 服务器对用户进行认证，返回 RADIUS ACCESS ACCEPT（如果认证通过）报文到 NAS，NAS 完成相应操作允许用户接入，同时发送 EAP-SUCCESS 报文到用户终端通知用户接入成功。

- 使用 EAP-TLS 方式进行身份验证：EAP-TLS 认证提供了一种基于证书的双向认证，除了在连接建立时主机和服务器之间分配的会话号（Session ID）之外，它需要通过安全连接在客户侧和服务器侧事先发布认证证书。EAP-TLS 既提供认证，又提供动态会话钥匙分发。RADIUS 服务器需要支持 EAP-TLS 认证，和认证证书的管理能力。TLS 支持双向认证，也就是网络（EAP-TLS 服务器）认证终端用户（Client），终端用户认证网络。只有在双向认证通过以后，服务器将向接入认证点发送 EAP-SUCCESS 消息，指示用户终端可以收发数据流。这个消息同时触发了对数据流的加密，在加密密钥建立之前，终端不发送数据。

6.1.2 认证流程

- 接收到 NAS 或 Portal 发送过来的认证请求；
- 检测其认证类型（PAP、CHAP、EAP-MD5、EAP-TLS）；
- 检测是否使用 Proxy；
- 查找数据库，进行数据检查，包括密码、安全认证等。首先查找单个用户在数据库中的满足情况，再查找该用户所在用户组在数据库中的满足情况；
- 通过数据检查后，看看是否需要地址分配；
- 如果需要地址分配，选择 AAA 自带的地址池或通过 DHCP 服务器进行地址分配；
- 这时，再去数据库中查找该用户及该用户所在的用户组是否需要携带返回的信息给 NAS；
- 返回成功。


注意

在认证过程中，任何一个环节出现检测错误，都将导致用户认证失败。

6.1.3 计费流程

- 接收到 NAS 或 Portal 发送过来的计费开始或计费结束请求；
- 检测是否使用 Proxy；
- 如果是计费请求，根据 Acct-Seesion-Id，UserName，NAS-IP-Address 等信息在数据库中查找是否已经存在该用户的上线记录，如果没有，则向数据库中插入该用户上线记录，如果只有该用户下线信息却没有上线信息，则修改这条记录；
- 如果是计费结束，根据 Acct-Seesion-Id，UserName，NAS-IP-Address 等信息在数据库中查找是否已经存在该用户的上线记录，如果没有，则向数据库中插入该用户下线记录，如果只有该用户上线信息却没有下线信息，则修改这条记录。有释放 IP 地址的记录，则再对 IP 地址进行释放；
- 发送计费响应给 NAS 或 Portal 服务器。

6.1.4 日志信息

可以通过日志信息了解一些用户认证拒绝的原因，如表 6-1 所述：

表**6-1** 日志信息

信息	原因
Access denied : The ×× attribute is not found!	AAA要求认证时携带属性××，而认证请求报文中没有携带该属性
The ×× value is incorrect!	认证请求报文中携带××属性的值不正确
Shared secret is incorrect!	AAA计算80属性错误
System inner error!	AAA分配内存失败，可能内存不足
System process timeout!	AAA处理超时
User[××] is not found!	AAA检测到用户××不存在，即数据库中没有该用户信息
System is busy!	由于配置原因，AAA不能再分配新的处理线程，可以适当增开新的线程
You are already logged in!	当AAA要求在同一时间内只允许某一用户在线个数为1个时，此时两个同用户名的用户同时上线，后者会被拒绝
You are already logged in n times!	当AAA要求在同一时间内只允许某一用户在线个数

信息	原因
	为n个时，此时 n＋1个同用户名的用户同时上线，第n＋1个用户会被拒绝
Invalid user!	认证请求中没有用户名
Invalid password!	认证请求中没有密码或检测为非法性
Auth type is rejected!	强制用户认证拒绝
Database query error!	数据库配置不正确导致，此时应检查相关数据库配置

6.1.5 数据库实现方式

AAA 服务器支持多种后台数据库，目前多使用 Mysql 和 Oracle 数据库。

AAA 服务器与 Mysql 的连接方式为调用 mysql 提供的 API（应用程序接口）进行连接；与 Oracle 的连接方式为调用 Oracle 提供的 OCI（Oracle 调用接口）进行连接。

数据库实现：

- 在 AAA 服务初始化时，需建立好多条与数据库（Mysql、Oracle 等）的连接通道，注意数据库地址、数据库用户名、数据库密码、数据库名称等的正确性；
- 建立连接队列；
- 当有请求时，从连接队列中获取一个空闲的连接，这样就占有了这个连接通道，可以通过该连接通道对数据库进行操作，操作后再将该连接放回队列中；
- 当队列中没有空闲的连接时，该请求会阻塞在这个队列上，一旦有空闲的连接，将获取连接。当有多个请求阻塞时，将会根据系统调度取决哪个请求获得空闲的连接；
- 当 AAA 服务关闭时，先释放连接队列，再释放连接通道。

进行配置时的注意事项：

- 需要用 AAA 服务器自带的地址池进行 IP 地址分配时，一定要统筹好地址分配方案，各地址池之间地址不可重叠；
- 在所有配置项设置完毕后，再使配置生效，因为生效配置的过程是不会处理任何认证、计费请求的，也就是说会中断业务操作；
- 如果使用 Oracle 数据库，可以事先进行一些优化，从而进一步提升 AAA 服务器的处理性能；
- 对于统计数据的刷新时间间隔不可过短，多少会影响一些 AAA 服务器的处理能力。

6.2 服务器运行状态

通过 AAA 服务器的‘服务器运行状态’显示，如图 6-1 所示，管理员可以查看总包数统计、认证包数统计、服务运行时间、线程统计和计费包数统计等信息。

图6-1 服务器运行状态

当前位置>>AAA服务器>>AAA服务器状态　　帮助>>

选择一个任务...

- 服务端状态查询
- 服务端配置
- 客户端配置
- 地址池配置
- 数据库配置
- 安全配置

总包数统计	
排队请求包数	24
处理请求包数	111
历史最多排队请求包数	28
丢弃请求包数	0

服务运行时间
34秒

线程统计	
历史最多线程数	30
当前线程数	26

认证包数统计	
排队认证包数	24
处理认证包数	111
历史最多排队认证包数	28
认证成功包数	111
认证失败包数	0

计费包数统计	
排队计费包数	0
处理计费包数	0
历史最多排队计费包数	0

统计数据 30 秒更新一次，点击刷新进行手动刷新。点击下面的“停止服务”可以停止AAA服务。

停止服务

6.2.2 总包数统计

1. 排队请求包数

排队请求包数是指 AAA 服务器接收到的正在队列中的请求包数。

2. 处理请求包数

处理请求包数是指 AAA 服务器接收到的已经处理完的请求包数。

3. 历史最多排队请求包数

历史最多排队请求包数是指 AAA 服务器接收到的队列中历史最大的请求包数。

4. 丢弃请求包数

丢弃请求包数是指 AAA 服务器丢弃的请求包数。

6.2.3 认证包数统计

1. 排队认证包数

排队认证包数是指 AAA 服务器接收到的正在队列中的认证请求包数。

2. 处理认证包数

处理认证包数是指 AAA 服务器接收到的已经处理完的认证请求包数。

3. 历史最多排队认证包数

历史最多排队认证包数是指 AAA 服务器接收到的队列中历史最大的认证请求包数。

4. 认证成功包数

认证成功包数是指经过 AAA 服务器处理，认证通过的请求包数。

5. 认证失败包数

认证失败包数是指经过 AAA 服务器处理，认证拒绝的请求包数。

6.2.4 服务运行时间

显示 AAA 服务器本次正常运行的累计时间。

6.2.5 线程统计

1. 历史最多线程数

历史最多线程数是指 AAA 服务器中历史最多存在过的处理线程个数。

2. 当前线程数

当前线程数是指 AAA 服务器中当前存在的处理线程个数。

6.2.6 计费包数统计

1. 排队计费包数

排队计费包数是指 AAA 服务器接收到的正在队列中的计费请求包数。

2. 处理计费包数

处理计费包数是指 AAA 服务器接收到的已经处理完的计费请求包数。

3. 历史最多排队计费包数

历史最多排队计费包数是指 AAA 服务器接收到的队列中历史最大的计费请求包数。

6.2.7 其它操作

1. 状态页面刷新

可以设置状态页面的刷新时间，缺省为 30 秒。刷新间隔还可设置为 15s、10s、5s。

也可以在需要查看 AAA 服务器最新状态时，点击‘刷新’链接，读取当前状态。

2. 停止服务

可以通过点击“停止服务”按钮，‘确认’后停止 AAA 服务器。

6.3 服务器端配置

通过 AAA 服务器的‘服务器端配置’，如图 6-2 所示，可以查看 AAA 服务器端的一些记录及 DHCP 服务器的配置。

图6-2 服务器端配置

AAA 服务器配置包括：

- 是否记录认证信息：配置是否将所有认证信息记录入日志。
- 是否记录认证失败信息：如果用户认证失败，是否对其认证失败的信息记录入日志。
- 是否启动 DHCP：是否使用 DHCP 来进行动态的地址分配策略。如果选否将使用 AAA 本身的地址池进行地址分配。
- DHCP 服务器地址：如果是使用 DHCP 服务器来进行动态的地址分配，那么请填写 DHCP 服务器的 IP 地址
- DHCP 服务器超时重传时间：AAA 服务器可以等待 DHCP 服务器处理请求的最大等待时间，默认值请参看用户管理界面的缺省值。
- DHCP 服务器超时重传次数：如果超时发生，那么 AAA 服务器可以重新向 DHCP 服务器请求 IP 地址的次数，默认值请参看用户管理界面的缺省值。

6.4 客户端配置

出于安全考虑，AAA 服务器可以接收从指定 NAS 上发送过来的认证或计费请求。如果有不属于客户端列表中的 NAS 向 AAA 服务器进行认证或计费，AAA 服务器将丢弃其请求包，不予响应。通过 AAA 服务器的‘客户端配置’，如图 6-3 所示，

可以实现此安全目的。

图6-3 客户端配置



6.4.2 添加客户端

在 NAS 地址一栏中，填入 NAS 的 IP 地址；在 AAA 验证密码一栏中填入 NAS 和 AAA 服务器双方认可的共享密钥；还可以在短名一栏中填入 NAS 的名字，以便记忆。最后点击“添加”按钮，将 NAS 地址加入到客户端列表中。


注意

在添加客户端时不要重复添加。

6.4.3 修改客户端

可以对客户端列表中的客户端进行配置修改。在客户端列表中选定要进行修改的客户端，该客户端的相应配置就会出现在右侧，此时就可以对其的配置进行修改，最后点击“修改”按钮完成修改。

6.4.4 删除客户端

可以对客户端列表中的客户端进行删除。在客户端列表中选定要进行删除的客户端，然后点击“删除”按钮进行删除。

6.4.5 重置客户端

将目前页面上填写的客户端配置信息清空，以便重新填写。

6.5 地址池配置

除了使用 DHCP 服务器来进行动态的地址分配外，AAA 服务器还可以用自带的地址池进行 IP 地址的动态分配。通过 AAA 服务器的‘地址池配置’，如图 6-4 所示，可以对 AAA 服务器自带的地址池进行管理配置。

图6-4 地址池配置

6.5.2 添加地址池

管理员可以自定义地址池。在“地址池名称”一栏中填写一个名称，以区别不同地址池。

“起始地址”一栏中填写地址池的起始地址；“终止地址”一栏中填写地址池的终止地址；“子网掩码”一栏中填写该地址池的子网掩码；如果有 DNS 服务器的话，可以在“DNS 服务器”一栏中填写其 IP 地址。

地址池可以与用户组建立对应关系。管理员可以在“可选用户组”中选择要添加的用户组，点击“添加组”按钮，该用户组的名称就会出现在“当前地址池对应用户组”列表中。相反，可以在“当前地址池对应用户组”中选择要删除的组，点击“删除组”按钮，该用户组的名称就会从“当前地址池对应用户组”列表中删除。这样，该地址池就可以对属于该用户组的用户进行动态 IP 地址分配了。

最后，点击“添加”按钮进行添加。

6.5.3 修改地址池

如图 6-4 所示，在左侧的“地址池列表”中选择要进行修改的地址池名称，该地址池的相关配置就会出现在右侧，此时就可以对其配置进行修改，最后点击“修改”按钮完成修改。

6.5.4 删除地址池

如图 6-4 所示，在左侧的“地址池列表”中选择要删除的地址池名称，该地址池的相关配置就会出现在右侧，然后点击“删除”按钮进行删除。

6.5.5 重置地址池

将目前页面上填写的地址池配置信息清空，以便重新填写。

6.6 数据库配置

通过 AAA 服务器‘数据库配置’，如图 6-5 所示，可以显示 AAA 服务器数据库的相关配置信息，其中包括“用户数据库地址”、“登录用户名”、“登录密码”及“确认登录密码”（密码信息显示的是不可读内容）。用户可以对这些配置项进行修改，需要注意的是，这些配置项必须配置正确，请用户配置的时候一定要谨慎。

图6-5 数据库配置



修改后，需要点击“保存并生效”按钮使之生效。

6.7 安全配置

通过 AAA 服务器‘安全配置’，如图 6-6 所示，可以配置系统的管理员，以保障管理员的安全性。只要在管理员列表中出现的管理员，都认为是可信和安全的。服务器端默认的‘管理员列表’配置为‘0.0.0.0’，表示服务器可接受来自任何主机的连接。

如果在‘管理员列表’中已添加管理员（‘0.0.0.0’自动删除），当有不属于该管理员列表中的管理员试图来访问是时，则服务器不接受其连接。

图6-6 安全配置

安全配置
安全配置 帮助>>
管理者列表
IP地址
192.168.0.55
0.0.0.0
192.168.0.55
添加 修改 删除

6.7.2 添加管理者

即添加可以连接服务器的管理者。方法是：输入管理者的 IP 地址后，点击“添加”按钮即可。


注意

当添加了一个管理者主机后，0.0.0.0 的 IP 自动被删除。

6.7.3 修改管理者

即对一个管理者进行修改，从“管理者列表”中选择需要修改的管理者，然后进行修改，最后点击“修改”按钮完成修改。

6.7.4 删除管理者

即对一个管理者进行删除，从“管理者列表”中选择需要删除的管理者，然后点击“删除”按钮进行删除。



不允许从管理者列表中删除本机的 IP。

6.7.5 重置管理者

恢复系统初始配置，重置管理 IP 地址为‘0.0.0.0’，表示可以接受任何 IP 地址的管理服务器的配置。

6.8 读取当前服务器配置

当用户想了解当前服务器的配置时，可以点击“读取当前服务器配置”按钮，这样，所有的当前配置就会显示在各个配置项中，一目了然。

6.9 保存并生效

管理员可以对本 AAA 服务器管理页面中的配置项进行配置，但是最后要进行保存生效。管理员在完成配置后，点击“保存并生效”按钮即可。



配置信息一经修改，原来的配置信息将不可还原。

7 Portal 服务器管理

7.1 概述

UniWorks UAS 系统的 Portal 服务器包括 Portal Web 服务器、Policy（COPS）服务器和 Portal 核心服务器。

对于 Web 用户，本系统必须配备 Portal 服务器，以实现 Web/Portal 认证。Web/Portal 认证是基于 HTTP 协议的认证方式，客户端不需安全任何软件，使用 Web 浏览器就可以进行认证，极大地方便了设备的安装实施。采用 Web/portal 认证，可以为用户提供基于时间和流量的计费方式，提供基于用户的带宽管理和有效性检测。

UniWorks UAS 的 Portal 服务器中包含一个 Policy（COPS）服务器，实现了 COPS 协议的策略服务器，即从 COPS 协议上考虑 Portal 服务器就是一个 PDP。Portal 服务器当与实现了 COPS 协议的 PEP（港湾网络有限公司的 PowerHammer ESR 系列路由器已经实现了该协议）一起部署应用时，可以实现对认证用户的策略化管理，如用户的 ACL、QoS 等。

Portal 核心服务器维护上网用户 Session Pool，和 AAA 服务器、Policy 服务器和 Portal Web 服务器配合完成 Web 用户上线、下线、异常下线检测和 ESR 设备 Session Pool 同步等核心逻辑流程。

通过 Portal 服务器管理，管理员可以监控 Portal 服务器和 Policy 服务器的运行状态；配置 Portal 服务器和 Policy 服务器的运行参数；并提供查询在线用户，与 PowerHammer ESR 系列路由器同步等 Portal 相关的管理操作。

7.2 Portal服务器状态

通过 Portal 服务器‘Portal 服务器状态’，如图 7-1 所示，管理员可以查看上线人数、服务运行时间和排队状态等信息。

图7-1 Portal 服务器状态

当前位置>>portal服务器>>portal服务器状态 帮助>>

上线人数	
通过web上线人数	0
通过802.1x上线人数	0
通过PPPoe上线人数	0
总上线人数	0

服务运行时间
0天1时18分32秒

排队状态	
排队请求WEB登录人数	0
排队请求WEB下线人数	0

统计数据 30 秒更新一次，点击刷新进行手动刷新。点击下端的“停止服务”可以停止Portal服务。

停止服务

7.2.2 上线人数

Portal 服务器中维护着通过各种登录方式上线人数的状态。

1. 通过 Web 上线人数

通过 Web 方式登录的在线人数。

2. 通过 802.1x 上线人数

通过 802.1x 方式登录的在线人数。

3. 通过 PPPoE 上线人数

通过 PPPoE 方式登录的在线人数。

4. 总上线人数

各种登录方式在线人数总和。

7.2.3 服务运行时间

显示 Portal 服务器本次正常运行的累计时间。

7.2.4 排队状态

1. 排队请求 **Web** 登录人数

以 Web 方式登录，正在排队处理中的人数。

2. 排队请求 **Web** 下线人数

以 Web 方式下线，正在排队处理中的人数。

7.2.5 其它操作

1. 状态页面刷新

可以设置状态页面的刷新时间，缺省为 30 秒。刷新间隔还可设置为 15s，10s，5s。

也可以在需要查看 Portal 服务器最新状态时，点击‘刷新’链接，读取当前状态。

2. 停止服务

可以通过点击“停止服务”按钮，‘确认’后停止 Portal 服务器。

7.3 Portal服务器配置

Portal 服务器配置如图 7-2 所示：

图7-2 Portal 服务器配置

Portal服务器配置 帮助>>		
AAA服务器地址	10.5.4.34	(不要使用127.0.0.1和localhost)
AAA验证密码	testing123	
Policy服务器地址	10.5.4.34	(不要使用127.0.0.1和localhost)
心跳信号时间间隔	30	秒
客户端重试次数	8	
客户端超时时间	10	秒

2. AAA 服务器地址



如果已经在管理服务器首页中配置了 AAA 服务器的地址，此处将会自动取用已配置的 AAA 服务器地址。

Portal 服务器将以此地址做为所有 RADIUS 请求的目的地址。



一定不要配置成 127.0.0.1 或 localhost。

3. AAA 验证密码

AAA 验证密码，必须和 AAA 服务器的相应配置保持一致。

4. Policy 服务器地址

Policy 服务器和 Portal 服务器一般运行在同一台机器上。



Policy 服务器地址将会自动取用系统的 Portal 服务器 IP 配置。



一定不要配置成 127.0.0.1 或 localhost。

5. 心跳信号时间间隔

Web 用户异常下线心跳信号检测间隔，取值范围为 30－3000 秒，默认值请参看管理界面给出的数值。

6. 客户端重试次数

发送 RADIUS 请求的失败重试次数，取值范围为 0－10 次，默认值请参看管理界面给出的数值。

7. 客户端超时时间

发送 RADIUS 请求的超时时间，取值范围为 8－300 秒，默认值请参看管理界面给出的数值。

7.4 Portal安全配置

用来配置可以对此 Portal 服务器进行管理的管理服务器的 IP 范围，允许的 IP 在管理者列表中显示。默认的 IP 配置是 0.0.0.0（表示允许所有 IP 的管理服务器进行连接），输入的 IP 地址形式为 x.x.x.x，不能为网段格式。

7.4.1 添加管理者

在 IP 地址项中加入管理服务器的 IP 地址，然后，点击‘添加’按钮，IP 地址就会添加到左边的管理者列表文本框中。可以添加多个，添加完毕后点击‘确定’按钮。



添加了非 0.0.0.0 的管理 IP 后，则对管理服务器 IP 有了限制。代表所有主机都能访问的 0.0.0.0 配置将会被自动删除。

7.4.2 修改管理者

选中欲修改的管理者 IP，在 IP 地址文本框中输入新 IP 地址，然后点击‘修改’按钮，完成修改。

7.4.3 删除管理者

选中欲删除的管理者 IP，单击‘删除’按钮，完成删除。



为了避免无法对 Portal 服务器进行管理，不允许将本管理服务器的 IP 删除。

7.4.4 重置管理者

恢复系统初始配置，重置管理 IP 地址为‘0.0.0.0’，表示可以接受任何 IP 地址的管理服务器的配置。

7.5 Policy服务器状态

通过‘Policy 服务器状态’，管理员可以查看当前有效的 Portal 连接、当前有效的 COPS 客户端连接等信息，如图 7-3 所示：

图7-3 Policy 服务器状态

当前有效的Portal连接	
Portal服务器IP地址	10.5.4.144

当前有效的COPS客户端连接	
PEP ID	PEP IP地址
harbourPep	10.5.4.153

7.5.2 当前有效的Portal连接

表示当前连接到 Policy 服务器的 Portal 服务器地址。该连接在同一时间内只有一个生效，即在同一时间内 Portal 服务器和 Policy 服务器之间只会有一条有效连接。

如图 7-3 所示，表示当前连接到 Policy 服务器的有效的 Portal 服务器地址为 10.5.4.144。

7.5.3 当前有效的COPS客户端连接

如图 7-3 所示，显示的是当前连接到 Policy 服务器的 COPS 客户端 PEPID 和 IP 地址。Policy 服务器可以同时接收多个 COPS 客户端的连接。

7.6 其它操作

1. 状态页面刷新

可以设置状态页面的刷新时间，缺省为 30 秒。刷新间隔还可设置为 15s，10s，5s。

也可以在需要查看 Policy 服务器最新状态时，点击‘刷新’链接，读取当前状态。

2. 停止服务

可以通过点击“停止服务”按钮，‘确认’后停止 Policy 服务器。

7.7 Policy服务器配置

7.7.1 Policy基本配置

Policy 基本配置项包括：客户端 KeepAlive 时间和 PEPID 字符串，如图 7-4 所示：

图7-4 Policy 基本配置

Policy服务器配置 帮助>>

客户端KeepAlive时间 120 （秒）

PEPID字符串名称列表 harbourPep

名称:

发送keyID key:

接收keyID key:

添加 修改 删除

2. 客户端 KeepAlive 时间

客户端 KeepAlive 时间是指 COPS 客户端（ESR 设备）定期向 Policy 服务器发送 KeepAlive 报文的时间间隔，取值范围是 60-600 秒，默认值请参看管理界面给出的数值。

3. 添加 PEPID 字符串

(1) 需要在‘名称’输入框中输入 PEPID 的字符串名称，该‘名称’用来限制可以连接到本 Policy 服务器的 COPS 客户，只有添加到‘PEPID 字符串名称列表’中的 PEPID 才能连接到本 Policy 服务器。



提示

‘名称’输入限制为 30 个字符，并且要求该名称由字母、数字和下划线组成。

(2) 发送 key 是指 Policy 服务器在向 COPSClient 发送报文时通过 HMAC 算法进行消息摘要运算时使用的字符串。发送 keyID 是指在传送的报文中指明 Policy 服务器对所发送的报文进行消息摘要运算时使用的 key 的标识符，所以 keyID 和 key 要成对使用，是一对一的关系，而且只有在 COPSClient 的接收 keyID 和接收 key 与 Policy 服务器的发送 keyID 和 key 相一致时 Policy 服务器才能和 COPSClient 正常通信，否则对方会拒绝接收 Policy 服务器的报文。keyID 的输入范围是 1－65535 中的任意一个整型数，key 为最长 32 字符长的字符串，并且由字母、数字和下划线组成。

(3) 接收 keyID 和 key 的概念和发送 keyID 和 key 基本一样，只不过它是指接收 COPSClient 的报文时进行消息验证用的字符串和字符长标识符，要求只有和 COPSClient 配置的发送 keyID 和 key 相一致时才会和 COPSClient 进行正常的通信。由于 Policy 服务器可以接收多个 COPSClient 的连接，所以它支持多个 keyID 和 key 的组合对。它们的输入范围和发送 keyID 和 key 的要求一样。多个 keyID 和 key 的组合对之间用分号分隔，如 1 abc；2 def。

对于添加 PEPDI 字符串要求要正确填写上面所提到的三个内容，填写完毕后选择‘添加’按钮即可完成操作。

4. 修改 PEPID 字符串

在 PEPID 名称字符串列表中选择准备修改的 PEPID，然后在图中所示的右侧的输入框中输入新的内容后选择‘修改’按钮即可完成操作。

5. 删除 PEPID 字符串

在 PEPID 名称字符串列表中选择准备删除的 PEPID，然后选择‘删除’按钮即可完成操作。

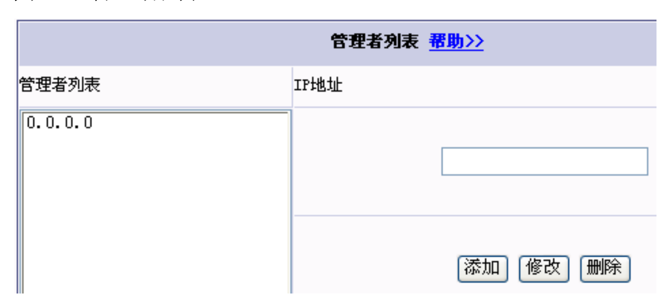
6. 重置 PEPID 字符串

将目前页面上配置的 PEPID 字符串清空，以便重新输入。

7.7.2 Policy安全配置

管理员可以通过‘管理者列表’对 Policy 服务器的管理服务器地址进行配置，从而实现 Policy 服务器的安全管理。如图 7-5 所示：

图7-5 管理者列表




提示

默认情况下为 0.0.0.0，表示任何的管理服务器皆可以对 Policy 服务器进行配置管理。

2. 添加管理者

在图 7-5 所示的‘IP 地址’输入框中输入允许管理 Policy 服务器的管理服务器的 IP 地址，然后选择‘添加’按钮即可。如果当前管理列表中只有 0.0.0.0，则添加指定的 IP 地址后将会把‘0.0.0.0’管理者自动删除，同时如果此时添加的 IP 地址为非本地 IP 地址，则自动将本地的 IP 地址添加到管理者列表中。

3. 修改管理者

选定‘管理者列表’中将要修改的 IP 地址后，在‘IP 地址’输入框中输入新的管理服务器的 IP 地址，然后选择‘修改’按钮即可生效，如果需要修改的 IP 地址为本地的 IP 地址则会提示出错，拒绝更改。

4. 删除管理者

选定‘管理者列表’中需要删除的 IP 地址后，选择‘删除’按钮即可生效。对于本地的管理地址删除会提示出错，拒绝删除。

5. 重置管理者

恢复系统初始配置，重置管理 IP 地址为‘0.0.0.0’，表示可以接受任何 IP 地址的管理服务器的配置。

7.8 读取当前服务器配置

向后台服务器发送请求，将服务器当前的配置信息读取到管理服务器上，并以此为依据刷新当前管理页面。

7.9 保存并生效

通知后台服务器保存并立即应用当前的配置项。

7.10 查询在线用户状态

通过‘查询在线用户状态’，管理者可以通过选择用户名、上线时长、NAS 端口、NASIP 地址等条件进行 Portal 服务器中的在线用户状态查询，如图 7-6 所示：

图7-6 查询在线用户状态




提示

1、这些条件是“与”的关系。例如：查询用户名为 user，并且上线时长大于 1 小时的在线用户。

2、这些条件均为可选项，如果各项都保持空白表示查询 Portal

中所有的在线用户。

7.11 与ESR同步

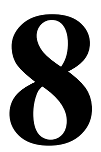
由于网络异常或其它一些不确定的因素，会导致 Portal 服务器和 ESR 设备中的在线用户状态不一致。Portal 服务器提供了自动定时同步的机制。方法是：选择“与 ESR 同步”选项，然后，点击‘确定’。这时，管理服务器就会向 Portal 服务器发出同步请求，Portal 服务器接收到同步管理请求后会立即执行与 ESR 设备的数据同步操作。



提示

管理服务器在成功发送同步请求后，会立即返回“已发送同步命令至服务器”的提示页面。但是这并不代表同步已经成功的完成，此时实际的 Portal 服务器与 ESR 设备之间的数据同步可能还在处理中。

您也可以在管理界面中手动同步 Portal 服务器和 ESR 设备的在线用户会话池。



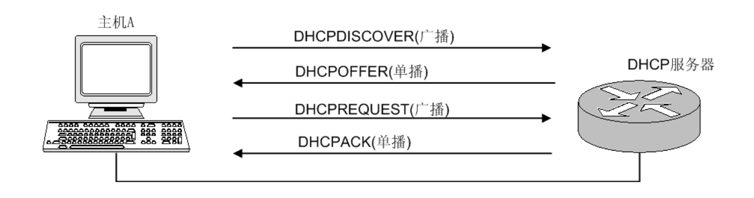
DHCP 服务器管理

8.1 概述

DHCP 的全称是动态主机配置协议（Dynamic Host Configuration Protocol）。UniWorks UAS 系统的 DHCP 服务器用于地址池配置和安全配置，其与 AAA 服务器配合完成统一地址分配功能。

在没有 AAA 服务器的网络环境下，DHCP 客户端从 DHCP 服务器申请 IP 地址的过程如图 8-1所示。客户端主机 A 先广播 DHCPDISCOVER 包寻找网络上的 DHCP 服务器，DHCP 服务器向客户端单播包含配制参数的 DHCPOFFER 消息。

图 8-1DHCP 客户端从 DHCP 服务器申请 IP 地址



- 当客户端第一次登录到网络时，它会向网络广播一个 DHCPDISCOVER 消息，此时由于客户端还不知道自己属于哪一个网路，所以封包的来源地址为 0.0.0.0，目的地址则为 255.255.255.255。
- 由于网络上可能不止一个 DHCP 服务器，凡是具有有效 IP 地址信息的 DHCP 服务器均从各自还没有租出的地址中选择一个空闲 IP，然后将该提议回应给客户端。
- 客户端从接收到的第一个提议中选定 IP 地址信息，并广播一条租用地址的消息请求。由发出该提议的 DHCP 服务器响应该消息，确认已接受请求并开始租用。
- 客户端收到确认后开始使用此地址。



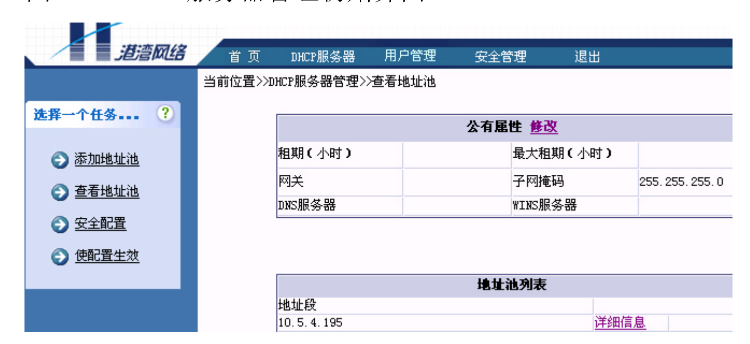
DHCP 客户端可以接收多个 DHCP 服务器的消息，自己从中选一个 DHCP 服务器，同时也暗示它拒绝了其它 DHCP 服务器应答的配制参数。

在本系统中，DHCP 服务器与 AAA 服务器配合完成统一地址分配功能过程是：

在用户认证时，如果用户通过密码校验并需要分配 IP 地址，则 AAA 服务器就会向 DHCP 服务器发送带有用户信息的特定的 DHCP 请求包。DHCP 服务器根据请求中的用户信息为此用户在相应地址池中分配一个 IP 地址，并回应 AAA 服务器的请求。同时，UniWorks UAS 系统的 DHCP 服务器除了响应 AAA 服务器的特定 DHCP 请求，也可以响应标准 DHCP 请求，从而使动态分配的 IP 地址统一在 UniWorks UAS 系统的 DHCP 服务器的管理之下，完成统一地址分配的功能。

通过‘DHCP 服务器管理’，如图 8-2所示，管理员可完成添加地址池、查看地址池、安全配置和使配置生效等操作。

图 8-2DHCP 服务器管理初始界面



8.2 添加地址池

‘添加地址池’用于为 DHCP 服务器添加一个或多个地址池。包括设置地址范围，配置所属组和配置路由、租期等属性。点击 ‘添加地址池’就会出现添加地址池界面，用户在完成地址段配置，所有组配置和属性配置之后，点击‘完成’按钮，将弹出确认对话框窗口，再点击‘确定’按钮即可完成添加地址池操作，并出现提示信息界面。

8.2.1 地址段配置

‘地址段配置’用于向地址池中添加一个或多个地址段，包括‘起始地址’和‘终止地址’。

1. 添加地址段

图 8-3添加地址段



如图 8-3所示，用户在右侧‘起始地址’和‘终止地址’处填入相应的 IP 地址后，点击‘添加’按钮，即可完成添加地址段操作。用户可以添加一个或多个地址段，图中左侧显示的就是已经添加的地址段。



1、地址段可为单地址（只有起始地址），各地址段不可重叠，也不可与已经配置的地址池的地址段重叠。

2、当用户输入的地址段重叠或输入的 IP 地址错误时，系统会提示出错信息。

2. 修改地址段

管理员在左侧已添加的地址段中选择需要修改的地址段，完成修改后，点击“修改”按钮，即可完成修改地址段操作。

3. 删除地址段

管理员在左侧已添加的地址段中选择需要删除的地址段，然后点击“删除”按钮，即可完成删除该地址段的操作。



对于服务器自身地址池，只包含服务器自身的 IP 地址，是 DHCP 自动初始化的，用户不能删除。

4. 重置地址段

将目前页面上配置的地址段信息清空，以便重新输入。

8.2.2 所有组配置

所有组配置用于配置该地址池为哪些用户组中的用户分配 IP 地址。如图 8-4所示，在右侧‘可选组’中列出了通过‘用户管理服务器’配置的所有用户组。有关用户组配置请参考第 9 章‘用户管理’的相关内容。其中“非 AAA 用户”组表示直接访问 DHCP 服务的用户组，也就是不通过 UniWorks UAS 系统 AAA 服务器认证的用户组，该组的地址池可以为标准 DHCP 客户端分配地址；“group1”、“group2”等为需要 AAA 服务器认证的用户配置的用户组。

图 8-4所有组配置界面



1. 添加地址组

用户在‘可选组’列表中选定某一组名，然后点击‘添加’按钮，即可完成添加组操作。该组名会出现在左侧‘允许分配地址组’列表中，同时该组名将从右侧可选组列表中删除。

2. 删除地址组

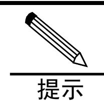
用户在‘允许分配地址组’列表中选定需要删除的组，然后点击“删除”按钮，即可完成删除地址组操作。

8.2.3 属性配置

‘属性配置’完成该地址池的某些私有属性配置。如图 8-5所示，用户可配置最大租期、租期、网关、子网掩码、DNS 服务器和 WINS 服务器属性，右侧列出的为公有属性。如果用户不配置该地址池的私有属性，该地址池将继承公有属性配置。

图 8-5属性配置界面

属性配置	私有属性	公有属性
最大租期（小时）		
租期（小时）		
网关		
子网掩码		255.255.255.0
DNS服务器		
WINS服务器		



最大租期及租期建议均配置为 120 小时；租期的配置不能超过最大租期的限定。

8.3 查看地址池

管理员通过‘查看地址池’可以查看 Uniworks UAS 系统 DHCP 服务器端配置的所有地址池和公有属性。如图 8-6所示：

图 8-6查看地址池

公有属性 修改			
租期（小时）		最大租期（小时）	
网关		子网掩码	255.255.255.0
DNS服务器		WINS服务器	

地址池列表		
地址段		
10.5.4.195	详细信息	
192.168.0.1-192.168.0.254	详细信息	删除
192.168.32.1-192.168.32.200	详细信息	删除

上方显示的是公有属性，下方地址池列表中显示的是各地址池的简要信息。

8.3.1 公有属性

公有属性是指作用于所有地址池的属性，包括最大租期、租期、网关、子网掩码、DNS 服务器和 WINS 服务器。点击‘修改’，管理员可对各属性进行修改。各属性说明如表 8-1所述：

表 8-1公有属性说明

公有属性	说明
最大租期	添加数字，范围为－1到99999，单位为小时，添加－1为无限期，即永久使用；如果不添，DHCP服务将使用默认值，最大租期默认值为24小时。
租期	添加数字，范围为－1到99999，单位为小时，添加－1为无限期，即永久使用；如果不添，DHCP服务将使用默认值，租期默认值为12小时。
网关	IP地址，如果不添，DHCP服务器将不设置该属性。
DNS服务器	IP地址，如果不添，DHCP服务器将不设置该属性。
WINS服务器	IP地址，如果不添，DHCP服务器将不设置该属性。
子网掩码	点分地址，默认值为255.255.255.0

8.3.2 地址池列表

地址池列表显示所有地址池的简要信息，并可查看某个地址池的详细信息或删除某个地址池。点击某个地址池右侧的‘详细信息’链接，可查看该地址池的所有地址段，允许使用的组和私有属性等信息，如图 8-7所示：

图 8-7地址池详细信息

地址段		允许使用的组	
192.168.0.1-192.168.0.254		group1 group2	
租期（小时）		最大租期（小时）	
网关		子网掩码	255.255.255.0
DNS服务器		WINS服务器	

点击某个地址池右侧的“删除”链接，可删除该地址池。

8.4 使配置生效

‘使配置生效’用于将先前的配置（包括添加的地址池、删除的地址池和修改的公有属性）在 UinWorks UAS 系统的 DHCP 服务器端正式生效，因为先前的操作只是修改 DHCP 服务的配置文件。方法是：点击 ‘使配置生效’，在系统弹出的确认对话框中点击‘确定’按钮，完成配置生效操作；如果点击‘取消’按钮则不作生效操作。

8.5 安全配置

UniWorks UAS 系统管理员可通过 DHCP 服务器的‘安全配置’，如图 8-8所示，配置能够操作 DHCP 服务器的管理员列表。

图 8-8安全配置




提示

‘管理者列表’中的‘0.0.0.0’为默认值，意为任意管理者，当用户添加管理者时将自动删除该默认值，并自动将本机 IP 地址添加到管理者列表。

8.5.1 添加管理者

在图 8-8所示的‘IP 地址’输入框中输入允许管理 DHCP 服务器的管理服务器的

IP 地址，然后选择‘添加’按钮即可。如果当前管理列表中只有 0.0.0.0，则添加指定的 IP 地址后将会把‘0.0.0.0’管理者自动删除，同时如果此时添加的 IP 地址为非本地 IP 地址，则自动将本地的 IP 地址添加到管理者列表中。

8.5.2 修改管理者

选定‘管理者列表’中将要修改的 IP 地址后，在‘IP 地址’输入框中输入新的管理服务器的 IP 地址，然后选择‘修改’按钮即可生效，如果需要修改的 IP 地址为本地的 IP 地址则会提示出错，拒绝更改。

8.5.3 删除管理者

选定‘管理者列表’中需要删除的 IP 地址后，选择‘删除’按钮即可生效。对于本地的管理地址删除会提示出错，拒绝删除。

8.5.4 重置管理者

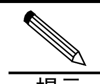
恢复系统初始配置，重置管理 IP 地址为‘0.0.0.0’，表示可以接受任何 IP 地址的管理服务器的配置。

9 用户管理

9.1 概述

用户管理是 UniWorks UAS 系统管理的一部分，管理 UniWorks UAS 系统中的用户数据。其用户管理功能包括：

- 查询用户
- 添加用户
- 批量添加用户
- 修改用户
- 删除用户
- 查询组
- 添加组
- 批量添加组
- 修改组
- 删除组


提示

有关帮助信息，管理员可通过“帮助”链接获取。

9.2 查询用户

进入用户管理界面后，选择“查询用户”链接，显示用户查询页面如下图所示：

图 9-1用户查询

用户名	
所属组名称	
同时在线限制	
NAS端口	
NAS IP	
用户 IP	
用户 MAC	
VLAN IP	
用户状态	○ 在线用户 ⊙ 全体用户

每页最大显示记录数 10

查询

管理员可根据用户名进行查询操作。查询结果为详细的用户信息。用户名支持“*”通配符形式，如：a*。

为了方便管理员操作，本系统支持用户的组合查询。管理员可输入一个或多个查询条件，输出为符合条件的用户的基本配置信息。若没有输入查询条件，则显示所有用户的配置信息。



提示

如果管理员想查询在线用户状态，可以选择“用户状态”中的“在线用户”条件。

在如上图的查询条件下，查询结果如下图所示：

图 9-2查询结果

用户名	所属组	服务类型				
a2	g1		详细信息	端口反查	修改	删除
a3	g1		详细信息	端口反查	修改	删除

刷 新　返 回　　总记录数：2　第1页/1页

点击某用户名对应的“详细信息”链接，即进入显示该用户详细配置信息页面，如下图所示：

图 9-3用户详细配置信息

用户申请信息表			
姓名	地址	证件类型	申请时间
李小明	北京市北三环厂洼街 zip=100086		2004-02-19 00:00:00
电话	E-Mail	证件号码	附注
1-10-68721722	xmli@sina.com	510010812340006	

用户配置信息表							
用户名	同时在线限制	NAS端口（允许）	NAS IP（允许）	用户 IP	用户 MAC	VLAN IP	认证类型
a2		15	1.1.1.1				

ACL策略配置表(缺省访问为：允许访问)			
协议类型	源端口	目的IP	目的端口
ANY	15	0.0.0.0/0	0

该用户尚无原始账单！

修 改 删 除 刷 新 返 回

管理员点击某用户名对应的"端口反查"链接可以进行用户接入交换机的端口反查。

9.3 添加用户

在用户管理页面选择'添加用户'链接，进入添加用户页面，如图 9-4 所示，管理员可根据系统提示逐条输入个人资料和配置信息，并完成对单个用户的添加。具体操作如下：

第一步：填写用户基本配置

图 9-4添加用户基本配置信息

用户名*	
密码*	
密码确认*	
所属组	
实时计费时间间隔	（必须大于60秒，建议大于600秒）
申请时间	2004-2-19

下一步 完 成 取 消

输入相关信息后，点击‘下一步’进入用户信息填写下一页；点击‘完成’将用户基本配置写入数据库。


提示

1、用户名和密码不能包含空格符。

2、‘*’ 处为必须填写内容。

3、要求实时计费的用户请配置实时计费时间间隔。实时计费时间间隔必须大于 60 秒，建议大于 600 秒。

第二步： 填写用户信息

图 9-5添加用户信息

用户名	a1
真实姓名*	
证件类型*	身份证
证件号*	
电话	
Email*	
地址	
邮编	地址和邮政编码请同时填写（香港：000000）
附注	

上一步　下一步　完 成　取 消

输入相关信息后，点击‘下一步’进入用户安全认证信息的配置页；点击‘完成’，将用户信息写入数据库。

第三步：填写用户安全认证配置信息

图 9-6添加用户安全认证信息

用户名	a1	
同时在线限制		
NAS端口		⊙ 允许 ○ 禁止
NAS IP		⊙ 允许 ○ 禁止
用户 IP		⊙ 允许 ○ 禁止
用户 MAC		⊙ 允许 ○ 禁止
VLAN IP		⊙ 允许 ○ 禁止
认证类型	Local / EAP / CHAP / PAP	

下一步 完 成 取 消

输入相关信息后，点击‘下一步’进入用户静态 IP 地址等的配置页；点击‘完成’，将用户安全认证配置信息写入数据库。


提示

1、建议填写安全配置属性。

2、认证类型默认值为空。若需要强制要求认证类型，可选择 local、EAP、PAP 或 CHAP 认证类型。

第四步：用户静态 IP 等的配置

图 9-7用户静态 IP 等的配置

用户名	a1
是否采用静态IP分配	⊙ 是 ○ 否
静态IP地址	
网关	
子网掩码	
DNS服务器	

上一步 下一步 完 成 取 消

采用静态 IP 分配是指用户可以选择不参加 AAA 服务器地址池中的地址分配，也不参加 DHCP 服务器的动态地址分配。输入相关信息后，点击‘下一步’，进入用户策略配置页面；点击‘完成’，将用户静态 IP 等配置信息写入数据库。

第五步：用户策略配置

图 9-8用户策略配置

访问控制列表

缺省访问控制类型： ⊙ 允许访问 ○ 禁止访问

ACL控制列表：

(访问控制类型与缺省类型相反)

协议类型: ANY

源端口:

目的IP地址:

目的端口:

添加 修改 删除 重置

QoS

上行带宽: M　上行突发流量: 4K

下行带宽: M　下行突发流量: 4K

上一步 完成 取消

点击‘添加’、‘修改’、‘删除’按钮可以操作右边选定的 ACL 配置项；点击‘完成’把配置信息写入数据库。至此，添加用户操作完成。


提示

1、IP 地址的格式为 IP/Mask，其中 IP 的输入格式为 x.x.x.x，掩码为 0-32 的数字。IP 地址默认为 0.0.0.0/0，表示匹配任意 IP。端口号为 0-65535 的数字，端口号为 0 表示匹配任意端口。

2、上行带宽和下行带宽取值范围为 1-1000M。上/下行突发流量有八个可选值（见下拉条选项），默认值为 4K。

9.4 批量添加用户

为了方便管理员实现批量用户的添加，本系统支持从文本文件导入用户，并完成添加的功能。文本文件由管理员创建或由数据库导出时自动创建。


注意

批量添加用户的文本文件名称和内容必须满足一定格式。

批量添加用户的文本文件的格式要求如下：

- **文件名**：扩展名为‘.db’，如：aaa_auth.db；
- **文件内容格式**：文本文件的每一行代表一个用户。不同用户之间用回车键隔开。

每一行用户信息必须满足如下格式：

- 用户名;密码;Attribute< 空格>op< 空格>Value;…<回车>

其中用户名，密码和用户基本属性（包括所属组名称、NAS 端口号、NASIP 地址等）之间用一个分号隔开。各项用户基本属性之间也用一个分号隔开。

在用户管理页面选择‘批量添加用户’，出现批量添加用户页面，管理员可通过选择文件，实现用户的批量添加。

9.5 修改用户

在用户管理页面选择‘修改用户’，出现修改用户页面，引导管理员输入用户名，确认后逐步对用户的个人资料和基本配置信息进行修改。



提示

用户个人信息、配置信息的修改方法与添加用户类似，在此不再冗述。

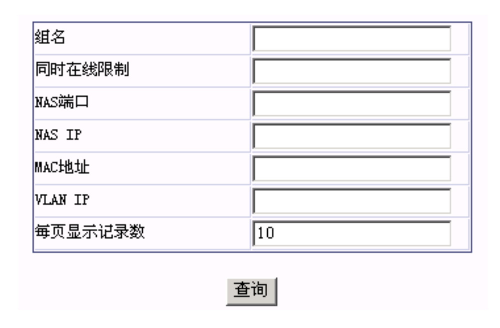
9.6 删除用户

在用户管理页面选择‘删除用户’，出现删除用户页面，引导管理员输入用户名，确认后将该用户的所有信息从数据库中删除。

9.7 查询组

在用户管理页面选择‘查询组’，显示组的查询页面如下图所示：

图 9-9查询组



管理员可根据组名进行查询操作。查询结果为详细的组信息。

为了方便管理员操作，本系统支持组的组合查询。管理员可以输入一个或多个查询条件，系统将输出所有符合条件的组，显示其基本配置信息。若无输入条件，则显示所有组。

9.8 添加组

在用户管理页面选择‘添加组’，出现添加组页面，如下图所示，管理员可逐条输入组的配置信息，并完成对单组的添加。

图 9-10配置组的属性





提示

1、组名不能包含空格符。

2、‘*’ 处为必须填写内容。

3、认证类型默认值为空。若需要强制要求认证类型，可选择 local、EAP、PAP 或 CHAP 认证类型。

4、选择允许 IP 分配使能，是指该组的所有用户均可采用 DHCP 服务器动态地址分配方式；如果该项配置选择为否，则该组的所有用户只能使用 AAA 服务器的地址池分配或使用静态 IP 地址。

点击‘下一步’，进行组的策略配置，如下图所示；点击‘完成’，将配置结果写入数据库。

图 9-11组的策略配置

访问控制列表

缺省访问控制类型： ⦿ 允许访问 ○ 禁止访问

ACL控制列表：

(访问控制类型与缺省类型相反)

协议类型： ANY

源端口：

目的IP地址：

目的端口：

添加 修改 删除 重置

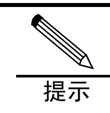
QoS

上行带宽： M 上行突发流量： 4K

下行带宽： M 下行突发流量： 4K

上一步 完 成 取 消

默认显示为数据库中原有的组策略配置。点击‘添加’、‘修改’、‘删除’按钮可以操作右边选定的 ACL 配置项。配置完成后点击‘完成’把组信息保存到服务器。至此，组添加操作完成。



1、IP 地址的格式为 IP/Mask，其中 IP 的输入格式为 x.x.x.x，掩码为 0-32 的数字。IP 地址默认为 0.0.0.0/0，表示匹配任意 IP。端口号为 0-65535 的数字，端口号为 0 的话表示匹配任意端口。

2、上行带宽和下行带宽取值范围为 1-1000M。上/下行突发流量有八个可选值，默认值为 4K。

9.9 批量添加组

为了方便管理员实现组的添加，本系统支持从文本文件导入组，并完成添加的功能。文本文件由管理员创建或由数据库导出时自动创建。



批量添加组的文本文件名称和内容必须满足一定格式。

批量添加组的文本文件的格式要求如下：

- 文件名：扩展名为‘.db’，如：aaa_group_auth.db；
- 文件内容格式：文本文件的每一行代表一个组。不同组之间用回车键隔开。

每一行组信息必须满足如下格式：

- 组名;Attribute< 空格>op< 空格>Value;…<回车>

其中组名和组基本属性（包括 NAS 端口号、NASIP 地址等）之间用一个分号隔开。各项组基本属性之间也用一个分号隔开。

在用户管理页面选择‘批量添加组’，出现批量添加组页面，管理员可通过选择文件，实现组的批量添加。

9.10 修改组

在用户管理页面选择‘修改组’，出现修改组页面，引导管理员输入组名，确认后逐步对组基本配置信息，组所包含用户，以及组所属地址池进行修改。修改组的管理页面及其功能类似于修改用户，在此不再冗述。

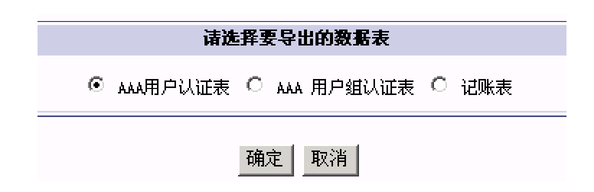
9.11 删除组

在用户管理页面选择‘删除组’，出现删除组页面，引导管理员输入组名，确认后将该组所有信息从数据库中删除。删除组的管理页面及其功能类似于删除单用户，在此不再冗述。

9.12 数据库导出

为了方便管理员实现数据库服务器中数据的导出，本系统支持用户认证表、用户组认证表以及用户账单表的导出。导出数据存放在文本文件中。用户可从管理服务器方便地下载并获得这些文件。数据库导出功能页面如下图所示：

图 9-12数据库导出



各数据库表导出的文件名分别为：

- AAA 用户认证表－aaa_auth.db
- AAA 用户组认证表－aaa_group_auth.db
- 记账表－aaa_acct.db

选择要导出的数据表，点击‘确定’后，将生成相应文本文件。此时出现如下提示信息，提示管理员下载并获得文件。

图 9-13下载文件



10 安全管理

10.1 概述

管理员通过‘安全管理’可以对管理服务器的安全参数进行配置和管理，主要包括管理员和密钥的配置和管理。

10.2 管理员列表

管理员是指能够登录管理服务器，并对连接到管理服务器的各个后台服务器（包括 AAA 服务器、Portal 服务器和 DHCP 服务器）进行管理的用户。只有超级用户（supervisor）能够对管理员用户信息进行设置。具体内容包括对现有管理员信息的查询显示、添加/删除管理员和修改管理员信息。

10.2.1 查询管理员信息

可通过查询现有的管理员列表，查看系统管理员的用户名和用户类型。如图 10-1 所示：

图 10-1管理员列表


当前位置>>管理员设置>>管理员列表

用户名	用户类型		
harbour	普通管理员	修改密码	☐
network	普通管理员	修改密码	☐
supervisor	超级用户	修改密码	☐

用户类型包括 Supervisor（超级用户，只有它可以进行安全管理的配置）和普通管

理员（只能进行各个服务器的管理操作）两大类。在‘管理员列表’中可以删除选定的普通管理员用户，超级用户不允许删除。

点击‘修改密码’链接可以修改管理员的密码。密码的最小长度为 16 个字符，最大长度为 64 个字符，而且不能包含空格。

10.2.2 添加管理员

添加一个新的管理员时需要输入管理员的用户名和密码。

10.3 密钥信息列表

密钥设置是对管理服务器和接受它管理的服务器之间的共享通信密钥进行配置，管理服务器和各个服务器依靠共享密钥来对它们之间传输的数据包进行校验，确认数据发送者的身份。出于安全考虑，密钥的长度应该在 16 到 64 个字符之间。密钥设置的项目包括密钥信息列表、添加/删除密钥和更改密钥。

10.3.1 查询密钥信息

密钥信息列表是显示管理服务器和接受它管理的服务器之间通信的共享密钥，显示内容包括服务器类型、IP 地址和共享密钥（明文形式显示）。在密钥信息列表中可以删除选定的密钥信息。

图 10-2密钥信息列表



当前位置>>密钥管理>>密钥信息列表 帮助>>

服务器类型	IP地址	共享密钥		
DHCP服务器	10.5.4.195	harbour_networks	修改密钥	☐
Portal服务器	10.5.4.17	harbour_networks	修改密钥	☐
AAA服务器	10.5.4.161	harbour_networks	修改密钥	☐
Policy服务器	10.5.4.17	harbour_networks	修改密钥	☐

删除

10.3.2 修改密钥

点击‘修改密钥’链接可以更改与这个服务器通信的共享密钥。



提示

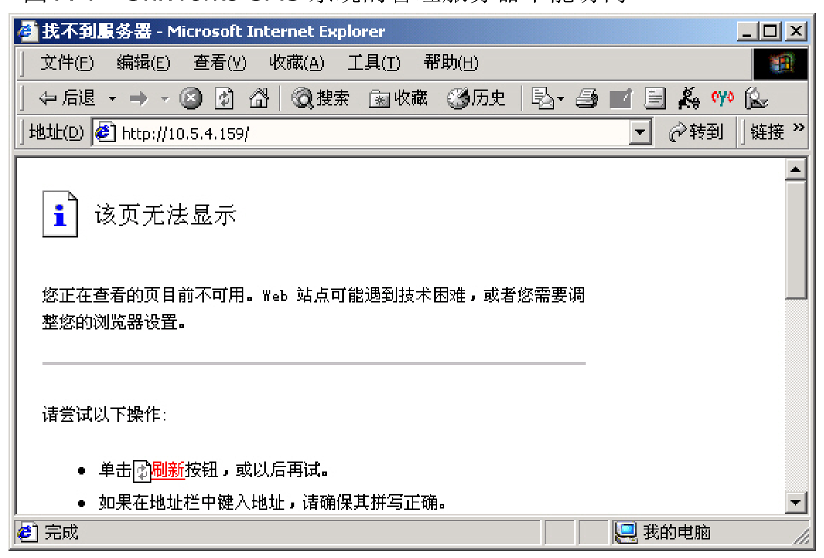
密钥的最小长度为 16 个字符，最大长度为 64 个字符（不能包含空格、%、?、='等符号）。

附录 常见问题处理

1. UniWorks UAS 系统的管理服务器不能访问

通过 Microsoft Internet Explorer6.0 访问时出现如图 A-1 所示情况，具体的原因应该是 Apache 后台服务没有启动，请先判断 Apache 服务是否正常运行（参见 2.4.2 节的相关内容）。如果没有正常运行，请使用/etc/init.d/apache start 命令启动 Apache 服务。

图 A-1 UniWorks UAS 系统的管理服务器不能访问



2. UniWorks UAS 系统不能通过管理服务管理 AAA 服务器

管理界面提示服务器连接不上。请检查 AAA 服务器 IP 地址配置是否正确或者 UniWorks UAS AAA 后台服务是否开启。

3. UniWorks UAS 系统不能通过管理服务进行用户管理

管理界面提示数据库连接不上。请检查用户管理服务器 IP 地址配置是否正确或者 Mysql 后台服务是否开启。

4. UniWorks UAS 系统不能通过管理服务管理 Portal 服务器

管理界面提示服务器连接不上。请检查 Portal 服务器 IP 地址配置是否正确或者 UniWorks UAS Portal 后台服务是否开启。

5. UniWorks UAS 系统不能通过管理服务管理 DHCP 服务器

管理界面提示服务器连接不上。请检查 DHCP 服务器 IP 地址配置是否正确或者 UniWorks UAS DHCP 后台服务是否开启。

6. ESR 设备不能通过 AAA 服务器认证

请检查 ESR 设备中的 RADIUS 共享密钥和相应的 AAA 服务器客户端中配置的共享密钥是否一致。


注意

ESR 设备中的 RADIUS 共享密钥必须和相应的 AAA 服务器客户端中配置的共享密钥一致。

7. 死账—用户不能下线

当只有上线用户，没有下线用户时，请检查 RADIUS Acct-On 报文选项是否打开。


注意

NAS 的 RADIUS Acct-On 报文选项一定要打开，这样才能保证在 NAS 重启时，会向 AAA 服务器发送 Acct-On 报文，使通过本 NAS 上线的所有用户下线，避免死帐的出现。命令行为:
config isp-domain <domain> accounting sync enable

8. Web 上线小窗口不能正常工作

请检查用户的 IE 游览器是否安装了 Google 工具栏等防止弹出窗口的工具，用户可卸载此类工具。



如果用户的 IE 游览器安装了 Google 工具栏等防止弹出窗口的工具，Web 上线小窗口将不能正常工作。

9. 两个以上不同账号同时通过 Web 上线

请检查 IE 浏览器是否设置了禁止 cookie 选项。如果用户的 IE 浏览器设置了禁止 cookie 选项，则不能保证用户 Web 上线的唯一性，即用户机器上可能会出现两个以上不同账号同时通过 Web 上线的情况。而正常情况下，一台机器上同时只允许一个账号 Web 上线。